

SafeSign Integration and Configuration Guide

For Check Point™ NG



This document contains information of a proprietary nature.

No part of this manual may be reproduced or transmitted in any form or by any means electronic, mechanical or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of A.E.T. Europe B.V.

Individuals or organisations, which are authorised by A.E.T. Europe B.V. in writing to receive this information, may utilise it for the sole purpose of evaluation and guidance.

A.E.T. Europe B.V.
IJsselburcht 3
NL - 6825 BS Arnhem
The Netherlands

Warning Notice

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

This information is subject to change as A.E.T. Europe B.V. reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances warrant.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement which accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL A.E.T. EUROPE B.V. BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

© Copyright A.E.T. Europe B.V., 2004. All rights reserved.

Safesign is a trademark of A.E.T. Europe B.V. All A.E.T. Europe B.V. product names are trademarks of A.E.T. Europe B.V.

Check Point, FireWall-1, VPN-1, VPN-1 Gateway, VPN-1 SecureClient, VPN-1 SecuRemote and OPSEC are trademarks, service marks, or registered trademarks of Check Point Software Technologies Ltd. or its affiliates.

Microsoft is a registered trademark of Microsoft Corporation. Windows and Windows NT are registered trademarks of Microsoft Corporation.

All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

Credit information:

This product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com)

This product includes software written by Tim J. Hudson (tjh@cryptsoft.com).

Contact Information: A.E.T. Europe B.V.

*IJsselburcht 3
NL-6825 BS
P.O. Box 5486
NL-6802 EL Arnhem
The Netherlands
Tel. +31-26-365 33 50
Tel. Support +31-26-365 35 43
Fax +31-26-365 33 51*



*info@aeteurope.nl | support@aeteurope.nl
<http://www.aeteurope.com/>
<http://www.safesign.com>*

SafeSign is a product developed by A.E.T. Europe B.V.

*Copyright © 2000 - 2004 A.E.T. Europe B.V.,
Arnhem, The Netherlands.
All rights reserved.*



Document Information

Filename: SafeSign Integration and Configuration Guide
For Check Point™ NG

Document ID: CheckPoint_SafeSign_v1.2

Project Information: Safesign User Documentation

Document revision history

Version	Date	Author	Changes
1.0	19-06-2003	Drs C.M. van Houten	First edition for SafeSign version 1.0.9.04
1.2	08-12-2004	Drs C.M. van Houten	Edited for SafeSign version 1.0.9.04-Update
1.2	07-05-2004	Drs C.M. van Houten	Edited for SafeSign Standard Version 2.0 for Windows

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

Table of contents

Warning Notice	I
Document Information	II
Table of contents	III
List of Figures	IV
About the Manual	VII
1 Introduction	1
1.1 Check Point™	1
1.2 SafeSign	1
2 Workstation Configuration and Connection	2
2.1 Requirements	2
2.1.1 Check Point	2
2.1.2 SafeSign	2
2.1.3 Smart card and smart card reader	2
2.2 Establishing a VPN Connection	2
3 Obtaining a certificate	12
3.1 Automatic Deregistration	12
3.2 Import a Digital ID	13
3.3 Generate a Digital ID using Check Point VPN-1 SecuRemote / SecureClient GUI	19
3.4 Generating a Digital ID issued by Microsoft CA	22
4 Setting up Checkpoint NG FP3 VPN-1 / FireWall-1	28
4.1 Obtain the CA certificate	28
4.2 Create CA Server	31
4.3 Generate a PKCS#10 Certificate Request	35
4.4 Request a Windows 2000 IPSEC certificate	41
4.5 Install IPSEC certificate for the Gateway	46
4.6 Configure IKE	48
4.7 Create new user	52
Index of Notes	a

List of Figures

Figure 1: VPN-1 SecureClient	3
Figure 2: Create New Site	3
Figure 3: VPN-1 SecureClient Authentication	4
Figure 4: VPN-1 SecureClient Authentication: Use Certificate	4
Figure 5: VPN-1 SecureClient Authentication: No token inserted	5
Figure 6: Certificate: User's certificate	5
Figure 7: Certificate: CA Certificate	6
Figure 8: Create New Site: Getting data from the site	6
Figure 9: SafeSign Login	7
Figure 10: SafeSign Login: wrong PIN	7
Figure 11: VPN-1 SecureClient: Negotiation failed	7
Figure 12: SafeSign Login: Token locked	8
Figure 13: VPN-1 SecureClient: IKE authentication failed	8
Figure 14: Verify Certificate	8
Figure 15: VPN-1 SecureClient: authenticated	9
Figure 16: VPN-1 SecureClient: Central Office	9
Figure 17: VPN-1 Secure Client: The certificate's private key not available	9
Figure 18: VPN-1 Secure Client: Negotiation has failed	10
Figure 19: VPN-1 SecuRemote: Certificate chain cannot be verified	10
Figure 20: VPV-1 SecureClient Connection	11
Figure 21: Digital ID Registration Status and Preferences: ONLINE	12
Figure 22: Token Management Utility: Token inserted	13
Figure 23: Token Management Utility: Import Digital ID	14
Figure 24: Import Digital ID	14
Figure 25: Import Digital ID: Select a Digital ID file	15
Figure 26: Import Digital ID: Digital ID file selected	15
Figure 27: Import Digital ID: Label on token	16
Figure 28: Import Digital ID: Digital ID password entered	16
Figure 29: Error: Digital ID needs a different password	16
Figure 30: Import Digital ID: Enter PIN	17
Figure 31: Import Digital ID: Working	17
Figure 32: Import Digital ID: The Digital ID has been imported successfully	17
Figure 33: Error: Key Size either smaller than 768 bits or larger than 1024 bits	18
Figure 34: Error: Token out of memory	18
Figure 35: VPN-1 SecuRemote: Create Check Point Certificate	19
Figure 36: Check Point Certificate: certificate storage type	19
Figure 37: Check Point Certificate: Cryptographic Provider	20
Figure 38: Create Check Point Certificate: Site address and registration key	20
Figure 39: SafeSign Login	21
Figure 40: Root Certificate Store	21
Figure 41: Check Point Certificate: Certificate created successfully	21
Figure 42: Microsoft certificate Services: Request a certificate	22
Figure 43: Microsoft Certificate Services: Choose Request Type	23
Figure 44: Microsoft Certificate Services: Advanced Certificate Requests	24
Figure 45: Microsoft Certificate Services: Certificate options	25
Figure 46: SafeSign Login	25
Figure 47: Microsoft Certificate Services: Certificate issued	26
Figure 48: Microsoft Certificate Services: Certificate installed	27
Figure 49: Microsoft Certificate Services: Welcome page CA	28
Figure 50: Microsoft Certificate Services: Retrieve the CA Certificate	29
Figure 51: Microsoft Certificate Services: Save this file to disk	30
Figure 52: SmartDashboard: New Certificate Authority	31
Figure 53: Certificate Authority Properties: General tab	32
Figure 54: Certificate Authority Properties: OPSEC PKI tab	32
Figure 55: SmartDashboard: Get Certificate Authority Certificate	33
Figure 56: SmartDashboard: Microsoft CA Server created	34
Figure 57: SmartDashboard: Network Objects	35
Figure 58: Check Point Gateway: VPN	36
Figure 59: Check Point Gateway: Certificate Properties	37
Figure 60: Generate Certificate Request	37
Figure 61: Generate Certificate Request successful	38
Figure 62: Check Point Gateway: Certificate Properties	39
Figure 63: Certificate Request View	40
Figure 64: Microsoft Certificate Services: Request a certificate	41
Figure 65: Microsoft Certificate Services: Choose Request Type	42

Figure 66" Microsoft Certificate Request: PKCS#10 request	43
Figure 67: Microsoft Certificate Services: Saved request	44
Figure 68: Microsoft Certificate Services: Download CA certificate	45
Figure 69: SmartDashboard: VPN	46
Figure 70: SmartDashboard: Certificate Properties	47
Figure 71: SmartDashboard: Topology	48
Figure 72: SmartDashboard: Traditional mode IKE Properties	49
Figure 73: SmartDashboard: Allowed certificates	50
Figure 74: Traditional mode IKE Properties	50
Figure 75: SmartDashboard: Global Properties	51
Figure 76: SmartDashboard: Users and Administrators	52
Figure 77: SmartDashboard: User Properties: General	53
Figure 78: SmartDashboard: User Properties: Groups	54
Figure 79: SmartDashboard: User Properties: Authentication	55
Figure 80: SmartDashboard: User Properties: Encryption	56
Figure 81: SmartDashboard: Install Database	57

About the Product

SafeSign is a software package that can be used to enhance the security of Internet applications that support hardware tokens through PKCS #11 and Microsoft CryptoAPI.

The SafeSign package provides a standards-based PKCS #11 Library and Cryptographic Service Provider (CSP), allowing users to store public and private data on a personal token, either a smart card or USB token. It also includes the SafeSign PKI applet, enabling end-users to utilise any Java Card 2.1.1 compliant card with the SafeSign middleware.

Combining full compliance with leading industry standards and protocols, with flexibility and usability, SafeSign can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers.

SafeSign allows users to initialise and use the token for encryption, authentication or digital signatures and includes all functionality necessary to use hardware tokens in a variety of PKI environments.

SafeSign Standard Version 2.0 for Windows supports the following tokens (as described in the product description):

- STARCOS SPK smart cards developed by [Giesecke & Devrient GmbH](#) (G&D): SPK2.3, SPK2.3 RawRSA, SPK2.4, SPK2.4 FIPS, and SPK2.5 Dual Interface (DI);
- The [Rainbow Technologies](#) iKey 3000 USB token with the completed STARCOS SPK 2.3 operating system;
- The Giesecke & Devrient StarKey100 USB token with the completed STARCOS SPK 2.3 / 2.4 operating system;
- Java Card v2.1.1 / OpenPlatform 2.0 compliant Java smart cards: Aspects OS755 v2.8, Axalto e-gate, Axalto Cyberflex Access Developer 32k, Axalto Cyberflex 64Kv1 and 64Kv2, G&D Sm@rtcafé Expert v2.0, G&D STARSIM Java, Gemplus GemXpresso 211pk/Pro R3, IBM JCOP 20/21/30/31, MartSoft Java card, Oberthur CosmopolIC v4, Orga JCOP 20/30.

SafeSign comes in a standard version with an installer for the following Windows environments¹:

- Windows 98 SE, Windows ME
- Windows 2000, Windows XP (Professional), Windows 2003 Server

In principle, SafeSign supports any PC/SC compliant smart card reader. However, to avoid power problems, smart card readers must be capable to provide at least a current of 60mA. PC/SC driver software is available from the web site of the smart card reader manufacturer. A.E.T. Europe is constantly seeking to extend the range of PC/SC smart card readers supported by SafeSign. Please contact us if you would like to find out about certifying your smart card reader.

For more information, refer to the latest SafeSign Product Description.

¹ Windows NT 4.0 is supported up to SafeSign 1.0.9.04

About the Manual

This manual is specifically designed for users of Check Point™, who wish to enhance the security of the Check Point™ products by the use of digital credentials stored on a SafeSign Token.

The manual describes how to obtain a certificate on the SafeSign Token and how to connect with your SafeSign Token to a remote site (protected by Check Point™ VPN-1® / FireWall-1®) by means of the Check Point™ VPN-1 SecuRemote™ and VPN-1 SecureClient™ application.

In order to set up your SafeSign Token for use with Check Point™ products, follow the instructions in the manual.

Every activity has a number of steps, indicated by the numbers at the left-hand side of the text. Each step will require you to take a certain action, which is indicated by a →.

Go through these steps and the actions you are required to take, in order to perform the desired activity, taking into account the notes in **blue**.

Note that this manual and in particular the integration and configuration portions of it, assume that you have installed SafeSign and have initialised the token with the SafeSign Token Management Utility, thus making it ready for use with Check Point™ VPN-1 SecuRemote™ and VPN-1 SecureClient™.

For instructions on installing SafeSign, see the *SafeSign User Guide for Installation*. For instructions on configuring and managing your SafeSign Token (including initialisation), see the *SafeSign Token Management Utility Guide / Token Administration Utility Guide*.

Though a complete discussion of the integration and configuration of Check Point™ VPN-1® / FireWall-1® is outside of the scope of this document, a brief overview of the steps required for configuration is provided, for guidance only, in [Chapter 4](#).

This document is part of the user documentation for SafeSign.

1 Introduction

1.1 Check Point™

VPN-1 Pro is the cornerstone of Check Point VPN-1 solutions, the most comprehensive set of products and technologies for remote access, intranet, and extranet VPNs. VPN-1 Pro protects the privacy of business communications over the Internet while securing critical network resources against unauthorized access.

FireWall-1 enables enterprises to define and enforce a single, comprehensive security policy that protects all network resources against attacks and unauthorized access. Its innovative architecture delivers a highly scalable solution that integrates all aspects of network security.

VPN-1 / FireWall-1 provides the ideal platform for enterprise VPN deployments, enabling encrypted communications and guaranteeing data privacy, integrity and authenticity. In addition to site-to-site VPN capability, VPN-1 / FireWall-1 Gateway deployments provide access to remote users when used with Check Point's VPN-1 SecureClient and SecuRemote software. Check Point's VPN-1 products support industry-standard algorithms and protocols, such as DES, 3DES, and IPSec/IKE. Digital certificate support is included for organizations with Public Key Infrastructure (PKI) deployments.

1.2 SafeSign

While PKI and the use of digital certificates might be the solution to secure access through VPN, unauthorised persons may still access sensitive corporate resources from your computer, if such digital credentials are stored e.g. on your computer's hard disk. This is where the SafeSign token comes in: by placing your digital credentials on a token, security is achieved by secure two-factor authentication.

Secure two-factor authentication is based on something the user knows (the PIN for his token) and something the user has (the possession of his token). Even when someone would know the PIN of the token, he would not be able to get access, as he does not have the token and vice versa. Further advantages of the use of a token include portability and flexibility.

Using the SafeSign token in Check Point VPN-1 SecuRemote / SecureClient enhances security by storing a user's digital credentials (private / public key pair and X.509 certificate) on a PIN-protected token. Furthermore, the SafeSign software provides a flexible tool for personalizing the token and placing digital credentials on a token, taking maximum advantage of the possibilities offered by the Check Point VPN-1 / FireWall-1 solution with regard to digital certificates.

For remote access to a site secured by Check Point VPN-1 / FireWall-1, users simply have to insert the token and enter the password / PIN for the token when asked to do so. Credentials are exchanged and verified, and once the user is authenticated, he will be allowed to access the resources available to him.

2 Workstation Configuration and Connection

This chapter lists the requirements to use SafeSign tokens on a workstation to securely connect to a Check Point VPN-1 / FireWall-1 Gateway and describes how to create a new site in the Check Point VPN-1 SecuRemote / SecureClient and establish a VPN connection using the SafeSign token. It does not describe how to obtain a digital certificate, see for that purpose [Chapter 3](#).

2.1 Requirements

In order to use SafeSign tokens on a workstation to securely connect to a Check Point VPN-1 / FireWall-1 Gateway, the following requirements should be met.

2.1.1 Check Point

Check Point VPN-1 / FireWall-1 software that is configured to interact with and support local and remote workstations.

Check Point VPN-1 SecuRemote or VPN-1 SecureClient installed on each workstation.

This configuration and integration guide was created using Check Point VPN-1 SecuRemote / SecureClient NG Feature Pack 3, Build 52238.

2.1.2 SafeSign

Minimum SafeSign version to be installed is: SafeSign-STARCOS-1.0.9.04.

Current available SafeSign version: SafeSign Standard Version 2.0 for Windows.

Note that before being able to install SafeSign, you should have a PC / SC compatible smart card reader installed (unless you use the iKey 3000 USB token) and its appropriate drivers.

2.1.3 Smart card and smart card reader

SafeSign supports any PC/SC smart card reader, but is currently supported and tested with the smart card readers defined in the latest product description. Note that before being able to use smart card readers and smart cards, you should have Microsoft Smart Card Base Components and its update, the Smart Card Driver Library installed, for all non-Windows 2000 versions. Most smart card reader manufacturers include these in their driver package.

SafeSign supports a large number of tokens. For a complete overview, refer to the latest product description. Note that the token used should be initialised and contain a Digital ID to connect to a VPN site.

2.2 Establishing a VPN Connection



Requirements

Basic steps before setting up a connection, apart from the requirements above, include the import of the root certificate(s) and the preference to remove certificates from the certificate store when the token is removed.

The Token Management Utility does both: it allows the user to import and /or register root certificates and set the preference for the auto-removal of certificates from the certificate store when the token is removed.

This paragraph will assume that the root certificate(s) is available in the Microsoft Trusted Root Certification Authorities store and that SafeSign is configured to remove the user certificate from the Microsoft Personal certificates store.

For more details and configuration, see [Chapter 3](#).

When you have a Digital ID¹ on your token (which should be suitable for if not issued by the Check Point VPN-1 / FireWall-1 Gateway you are trying to connect to), you can establish a connection with the Check Point VPN-1 SecuRemote / SecureClient software.

In this chapter, the application used to create a new site / connection, will be Check Point VPN-1 SecureClient.

When starting SecureClient, the following window will open:

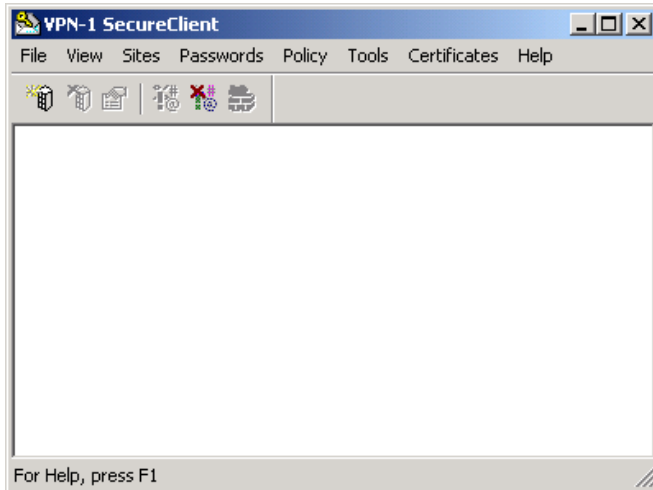


Figure 1: VPN-1 SecureClient

➔ Click **Sites > Create New Site**

This will open the *Create New Site* dialog:



Figure 2: Create New Site

➔ Enter the Name / IP address of the site and if desired, a nickname (e.g. Central Office as in this user guide) and click **OK**

¹ The term 'Digital ID' in this user guide refers to the combination of a private / public key pair and a certificate.

Upon clicking **OK**, the *VPN-1 SecureClient Authentication* dialog will open, allowing you to select the means of authentication to the site:

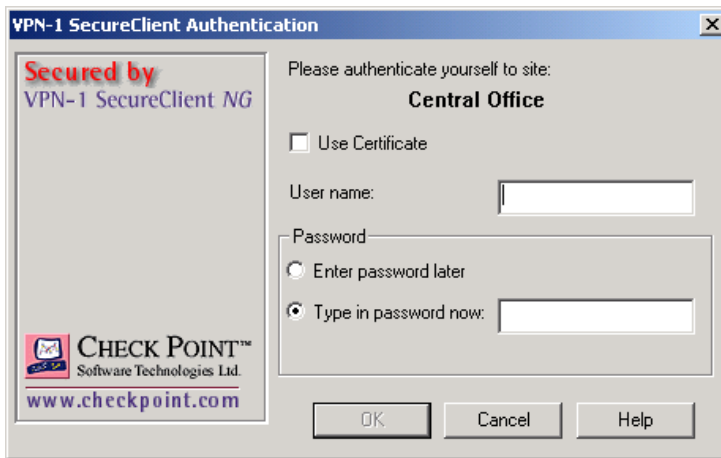


Figure 3: VPN-1 SecureClient Authentication

➔ Select the box **Use Certificate**

Upon selecting **Use Certificate**, a (drop-down) box will be displayed allowing you to select the certificate you want to use to authenticate yourself to the site:

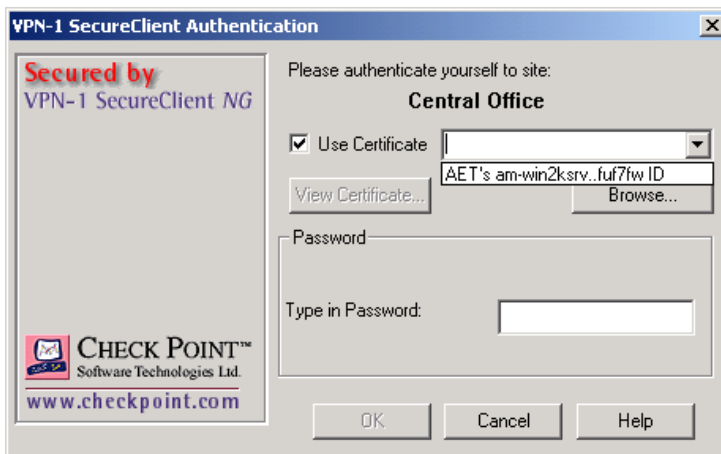


Figure 4: VPN-1 SecureClient Authentication: Use Certificate

➔ Select a certificate on the token¹ and click **OK**

¹ Note that all certificates in the certificate store are displayed; even those certificates that are not present on the token and that are not suitable for making the connection.



No Token

Make sure that your token is inserted at this point. If not and there are no other certificates in the certificate store, you will not be able to select a certificate:

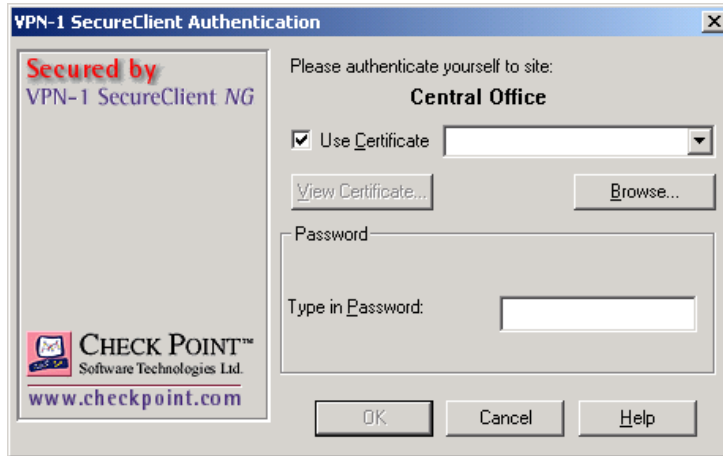


Figure 5: VPN-1 SecureClient Authentication: No token inserted

➔ **Cancel** this dialog and try again, after inserting a token



View Certificate

The button **View Certificate** allows you to view the content of the user and CA certificate, once you have selected a certificate:

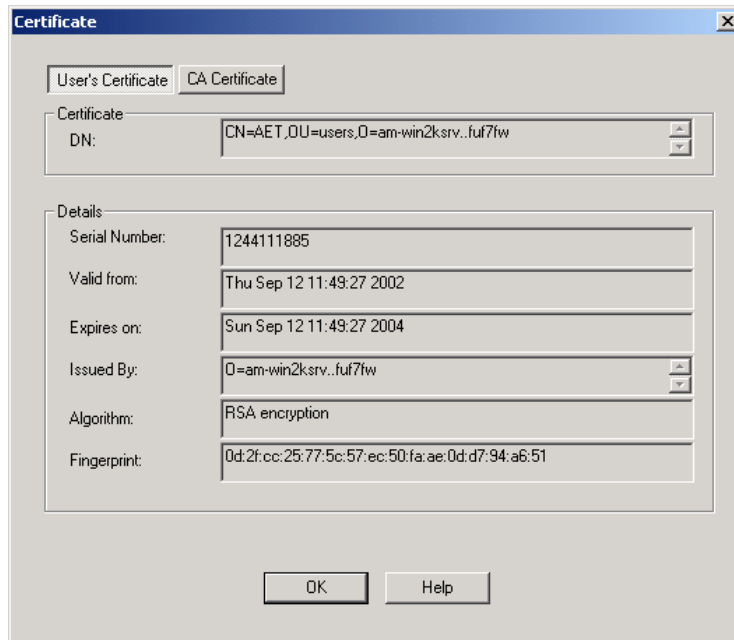


Figure 6: Certificate: User's certificate

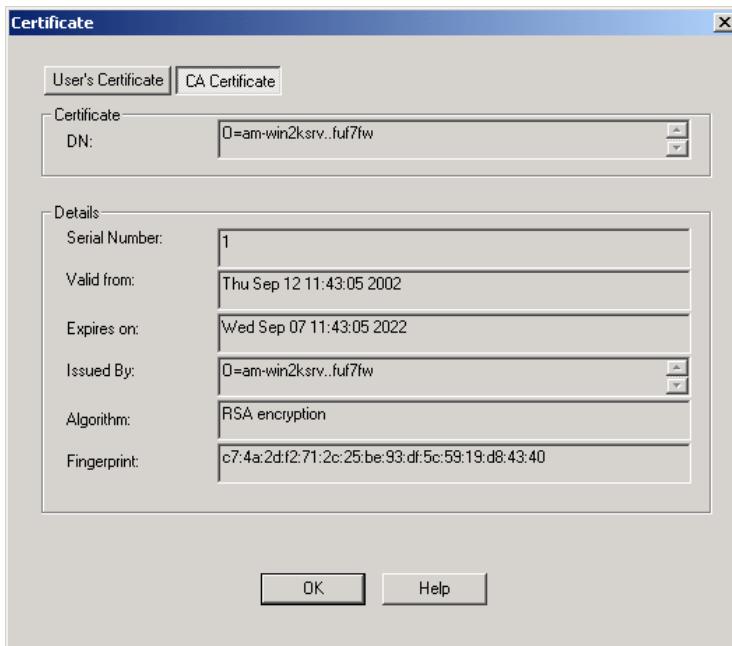


Figure 7: Certificate: CA Certificate

➔ Click **OK** to close the *Certificate* dialog box

Upon having selected a user certificate on the token in [Figure 4](#), data will be obtained from the site:

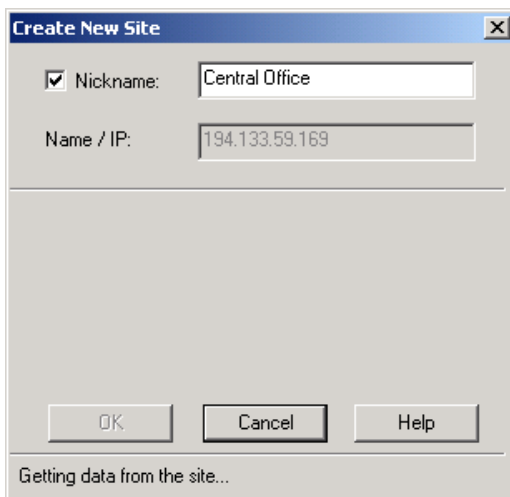


Figure 8: Create New Site: Getting data from the site

When the user has to be authenticated, i.e. his credentials should be checked, you have to log in to the token (that contains the credentials):

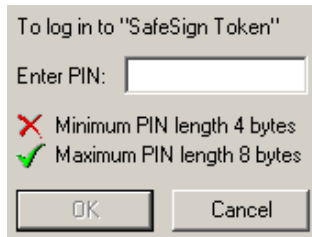


Figure 9: SafeSign Login

➔ Enter the PIN for your token and click **OK**



Incorrect PIN

When you enter an incorrect PIN at the *SafeSign Login* dialog, you will be informed:

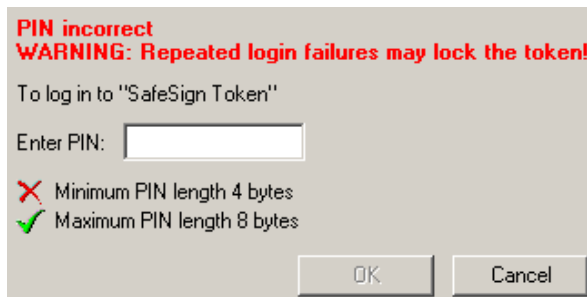


Figure 10: SafeSign Login: wrong PIN

➔ Enter the correct PIN and click **OK**



Cancel PIN

If you click **Cancel** in the *SafeSign Login* dialog, SecureClient will inform you that the connection failed:



Figure 11: VPN-1 SecureClient: Negotiation failed

➔ Click **OK** to close this dialog



Token Locked

When your token has been locked, i.e. after three wrong attempts to enter the PIN, SafeSign will inform you:



Figure 12: SafeSign Login: Token locked

- ➔ Click **OK** and use the Token Management Utility to unlock your token (see the *SafeSign Token Management Utility Guide / Token Administration Utility Guide*).

Upon clicking **OK** in the *Token locked* dialog, the VPN-1 SecureClient will inform you that the authentication failed:



Figure 13: VPN-1 SecureClient: IKE authentication failed

- ➔ Click **OK** to close this dialog

When the correct PIN has been entered ([Figure 9](#)), you will be asked to validate the site you are connecting to:

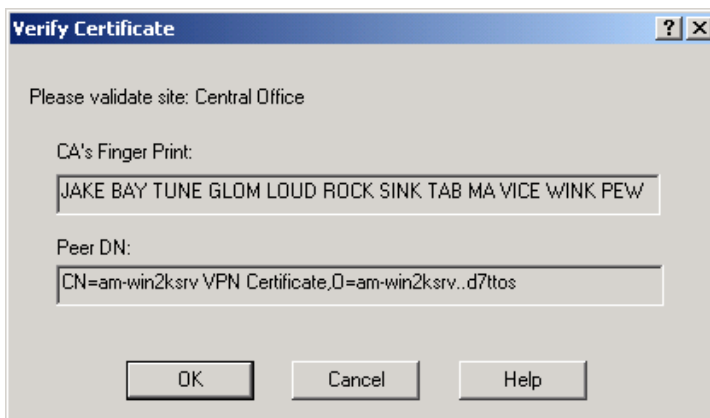


Figure 14: Verify Certificate

- ➔ Click **OK**

Upon clicking **OK**, you will be authenticated by the Check Point VPN-1 / FireWall-1 Gateway:

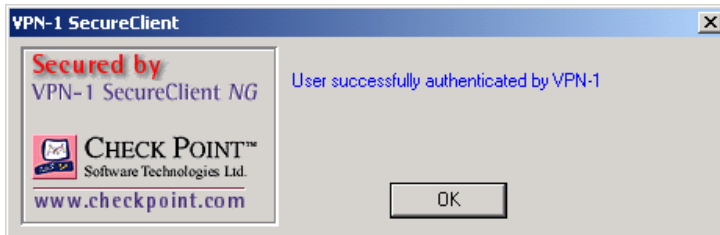


Figure 15: VPN-1 SecureClient: authenticated

➔ Click **OK** to close this dialog

A new site will now be created:

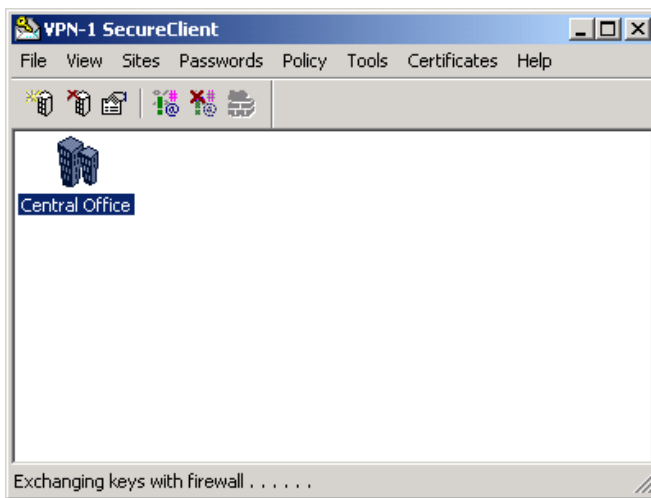


Figure 16: VPN-1 SecureClient: Central Office



Token Removed

When you remove your token after having logged in to it (and while validation and data exchange takes place), the Check Point VPN-1 SecureClient application will not be able to find your private key:

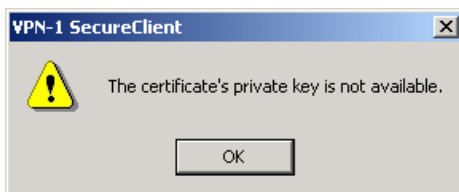


Figure 17: VPN-1 Secure Client: The certificate's private key not available



Wrong Certificate

When you have selected the wrong (i.e. unsuitable certificate, which the Check Point VPN-1 / FireWall-1 Gateway does not accept, either on the token or not), the following error will appear:

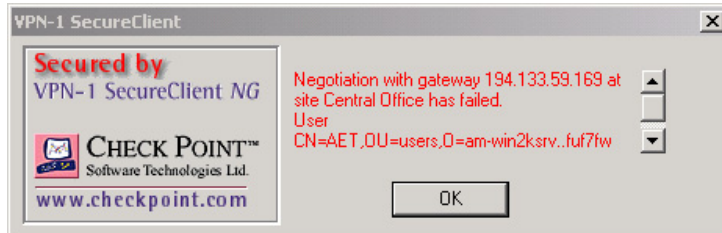


Figure 18: VPN-1 Secure Client: Negotiation has failed



Certificate Chain

When the certificate chain cannot be verified, i.e. the Root CA certificate is not in the list of Trusted Root Certification Authorities in the browser's certificate store or one or more of the certificates in the chain are not valid, the following dialog will appear upon attempting to create a connection:

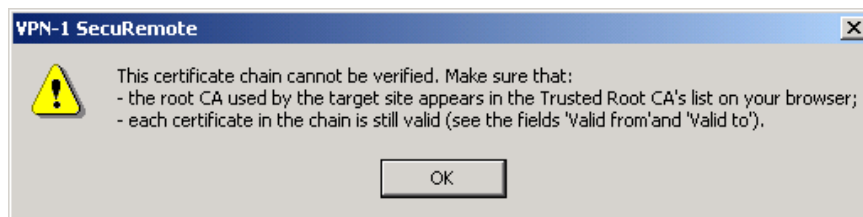


Figure 19: VPN-1 SecuRemote: Certificate chain cannot be verified

→ Click **OK** to close this dialog

Note that SafeSign is capable of registering root certificates if these are on the token.



Update Site

When you have already created a site, this site will be available in the *VPN-1 SecureClient* dialog. You can then update the site (**Sites > Update Site**) and use the **Connect** mode to connect directly to the site from the Check Point icon in the system tray (in order to do so, you will be asked for the PIN of your token by the *SafeSign Login* dialog):

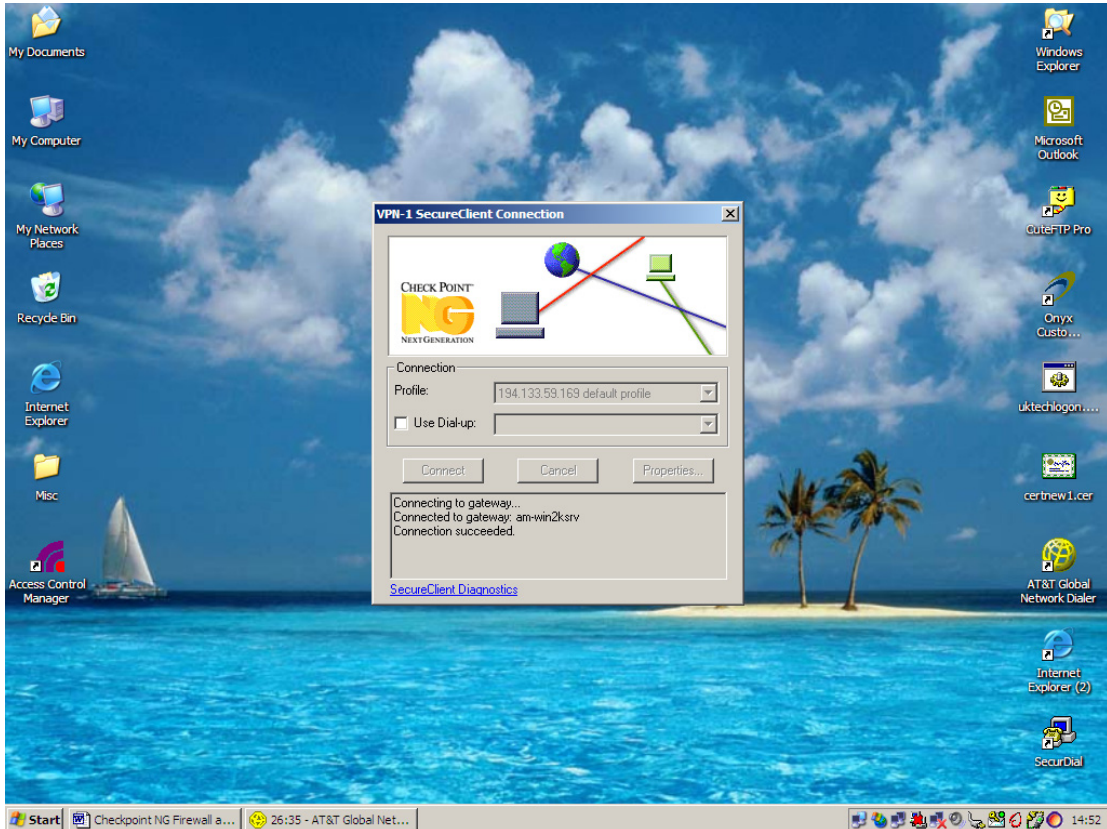


Figure 20: VPV-1 SecureClient Connection

This window will be minimized automatically once it is connected to the Check Point VPN-1 / Firewall-1 Gateway and there will be a green spot (instead of red in the picture above) on the Check Point icon on your system tray indicating that you are connected.

3 Obtaining a certificate

When you have installed SafeSign and you have initialised the token, you are ready to obtain a certificate.

Depending on the requirements of the Check Point VPN-1 / FireWall-1 Gateway you want to connect to, you can generate a key pair and download a certificate directly on the token or import a key pair and a certificate on the token.

This chapter will describe the following ways to obtain a certificate:

1. Import a Digital ID file in PKCS#12 format (a file that contains a certificate and the corresponding private key, protected with a password) generated and issued by the Check Point Internal CA (ICA) on the SafeSign token by means of the SafeSign Token Management Utility ([paragraph 3.2](#))
2. Generate a Digital ID (key pair and certificate) generated and issued by the Check Point Internal CA (ICA) on the SafeSign token by means of the Check Point VPN-1 SecuRemote / SecureClient application ([paragraph 3.3](#));
3. Generate a Digital ID (key pair and certificate) issued by the Microsoft CA on the SafeSign token through a web browser ([paragraph 3.4](#)).

[Paragraph 3.1](#) will first describe how to set SafeSign to automatically deregister certificate when the token is removed.

3.1 Automatic Deregistration

SafeSign can be configured to remove the user certificate from the Microsoft Personal certificates store.

The registration of both user and root certificates is handled by the SafeSign Certificate Registration Utility. Its settings can be configured in the SafeSign Token Management Utility.



Note

Certificate registration is not dependent on the SafeSign Token Management Utility being opened. The SafeSign Token Management Utility merely provides a means of configuring the settings of the Digital ID Registration, which is running as a process in the background.

In the SafeSign Token Management Utility, go to **Digital IDs > Registration Status and Preferences**. This dialog enables you to the status of the registration of certificates and set preferences for registration:

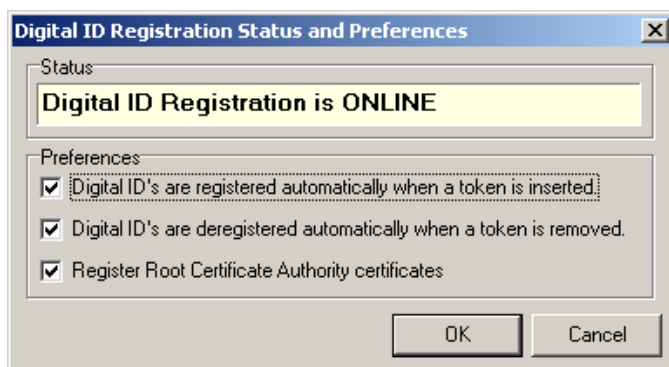


Figure 21: Digital ID Registration Status and Preferences: ONLINE

By default, all preferences are activated. Digital ID registration is online and will do the following:

- Digital IDs are registered automatically when a token is inserted;
- Digital IDs are deregistered automatically when a token is removed;
- Register Root Certificate Authority certificates.

You should ascertain the following to ensure a proper interoperability with Check Point VPN-1 SecuRemote / SecureClient:

Digital ID registration should be online: if the status of registration is offline (indicated in red lettering), registration will not work. You can activate registration by clicking **OK**.

The setting “Digital IDs are registered automatically when a token is inserted” should be activated: this will ensure that all certificates on the token will be registered when a token is inserted and are available for use.

The setting “Digital IDs are deregistered automatically when a token is removed” should be activated: This will ensure that certificates will be automatically deregistered from the Personal Certificates Store when the token is removed.

Enabling certificate removal when the token is removed will ensure that the certificate to be used for establishing a connection by means of Check Point VPN-1 SecuRemote / SecureClient will only be available when the token is inserted. Another important advantage of this feature is that in environments where computers are shared, no large amount of certificates is available in the certificate store (of users that may have used the computer at some time or other).

Note that the last option (“Register Root Certificate Authority certificates”) is a convenient feature, as the presence of the root certificate in the Trusted Root Certification Authorities store is a requirement for use of the Check Point VPN-1 SecuRemote / SecureClient. This option will ensure that any root certificate on the token will be registered in the root certificate store if it is not already present (ensuring flexibility, as the user will always have the complete certificate chain available).

3.2 Import a Digital ID

SafeSign allows you to import a Digital ID on your token and register it for use with applications that support the Microsoft CryptoAPI, such as Check Point VPN-1 SecuRemote / SecureClient.

This paragraph will describe how to import a Digital ID on your token through the SafeSign Token Management Utility.



Note

Note that the Digital ID(s) used in this manual to demonstrate how the import Digital ID process works are for demonstration purposes in this manual only.

The Token Management Utility is used as an example in this user guide (but the same applies to the Token Administration Utility).

Open the SafeSign Token Management Utility by selecting:

Start > Programs > SafeSign for STARCOS Version 1.0.9 > Token Management

The following dialog will open:

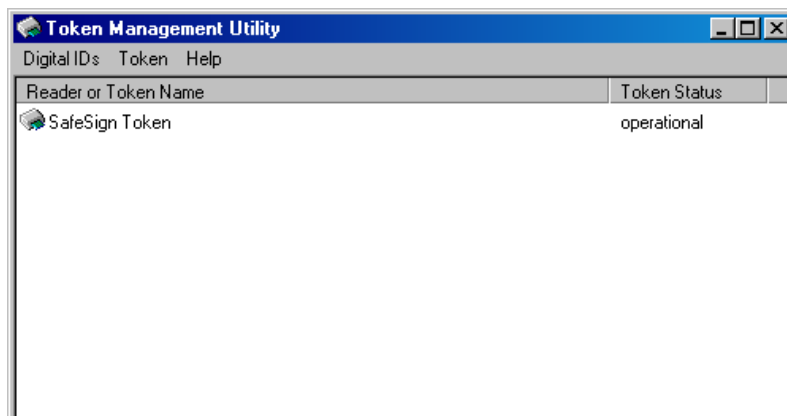


Figure 22: Token Management Utility: Token inserted

In the picture above, a token with the label “SafeSign Token” has been inserted in the reader and is operational.



Note

Make sure that your token has been initialised before you start importing or that it contains enough memory to import the Digital ID. If the label says “Blank Token – Uninitialised”, you should first initialise the token. If the token has a label, you may want to check if the token has enough space for the file you are about to import (this can be done in Token > Show Token Objects, where the total amount of total / free / used bytes are displayed).

1

To import a Digital ID, click **Digital IDs > Import Digital ID**:

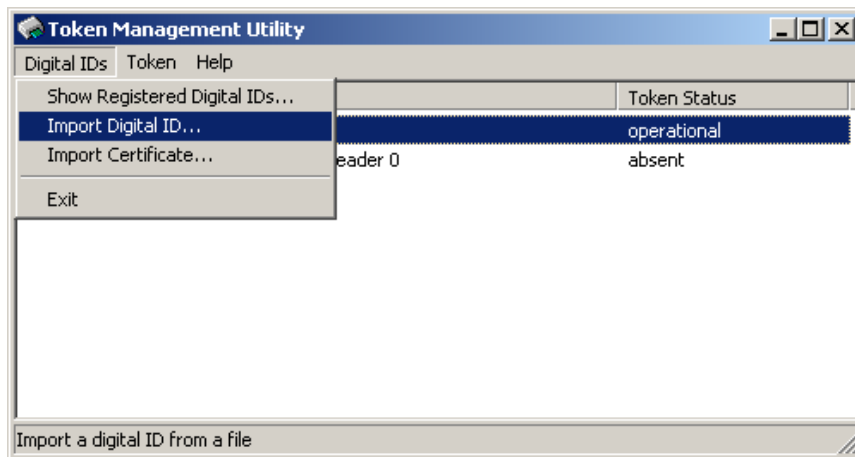


Figure 23: Token Management Utility: Import Digital ID

2

The following dialog will appear:



Figure 24: Import Digital ID

First, you will need to specify the location where the Digital ID file is stored. The Digital ID file can be stored anywhere, either on a hard disk or on a diskette.

Click on the symbol to select the location:

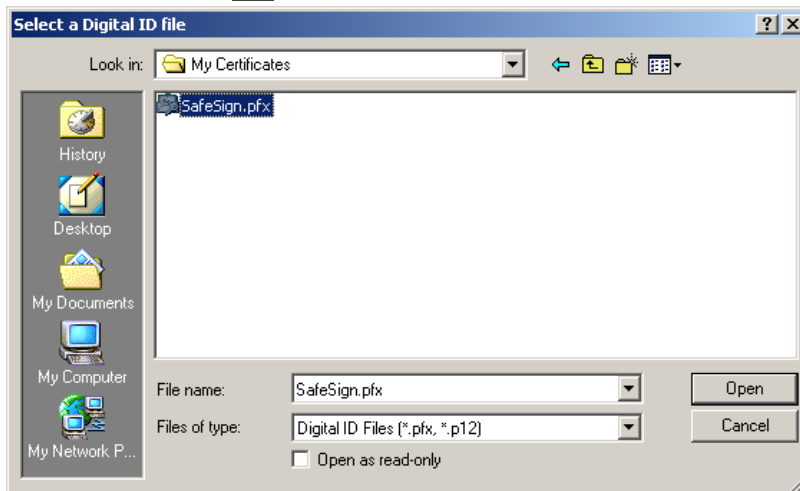


Figure 25: Import Digital ID: Select a Digital ID file

In the above example, the file was stored in: *C:/My Certificates*

➔ Select the Digital ID file by clicking on it, then click **Open**

The *Import Digital ID* dialog will now show the Digital ID file you have just selected:

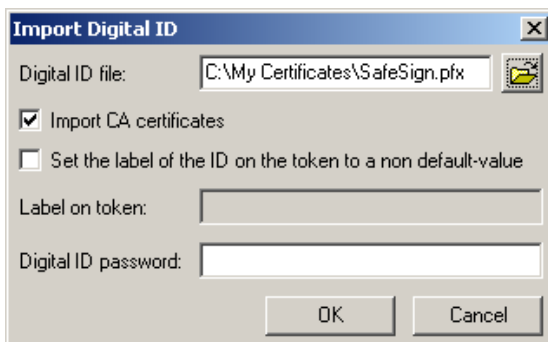


Figure 26: Import Digital ID: Digital ID file selected

➔ The next step is to enter the Digital ID password



Import CA certificates

When importing a Digital ID, you may choose whether you want to import the CA certificates as well. Doing so, will ensure maximum flexibility and interoperability. When taking your token to another computer (where the appropriate trust chain may not be installed), you always have all certificates with you and can register them.

Note that for Check Point VPN-1 SecuRemote / SecureClient, it is necessary that the certificate chain is present in the certificate store.

By default, the option **Import CA certificates** is selected.



Set the label of the ID on the token to a non default-value

When importing a Digital ID, the label of the Digital ID as set by the application used to obtain the Digital ID, will be copied. If you wish to set your own label to the Digital ID, select **Set the label of the ID on the token to a non-default value** and enter a label in the **Label on token** box, as illustrated below:

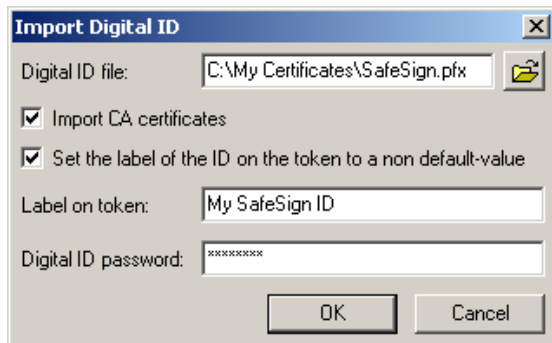


Figure 27: Import Digital ID: Label on token

3

Enter the password for the Digital ID file:

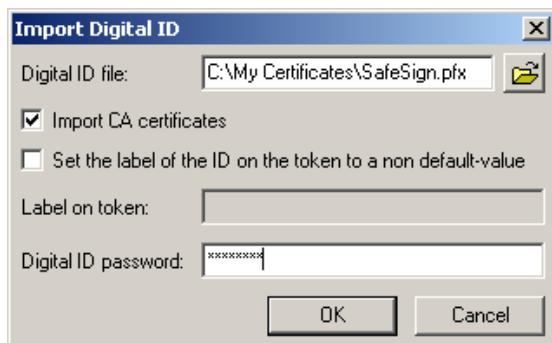


Figure 28: Import Digital ID: Digital ID password entered

This password will most likely be supplied to you by your Administrator.

➔ Click **OK** to import the Digital ID



Wrong Password

The password that you are requested to enter, is the password that was used to protect the Digital ID.

If you do not enter the correct password, the following prompt will be displayed:

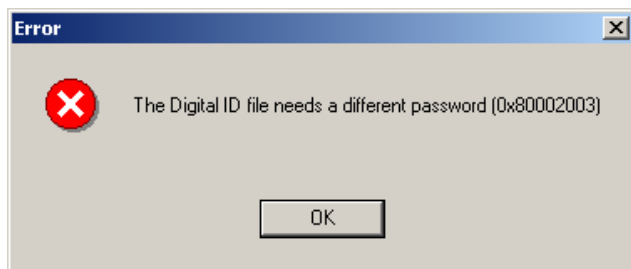


Figure 29: Error: Digital ID needs a different password

➔ Click **OK** to close this dialog box

You will have to start the import a Digital ID procedure again by clicking **Digital IDs > Import Digital ID**

4

When you have clicked **OK** after entering the correct password for the Digital ID file (Figure 28), you will be asked to enter the PIN for the token:

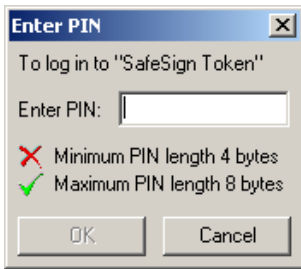


Figure 30: Import Digital ID: Enter PIN

→ Enter the correct PIN and click **OK**



PIN / PUK length

SafeSign enforces a minimum and maximum PIN / PUK length. If you enter a PIN / PUK of less than 4 characters or more than 8 characters, you will not be able to click the **OK** button in such instances where the PIN / PUK is required. Only when you enter a PIN / PUK of minimally 4 and maximally 8 characters, will the PIN / PUK be accepted. Note that the minimum / maximum PIN / PUK length may have been set to different values by the administrator.

5

Upon clicking **OK** after entering the correct PIN, the Digital ID will be imported:

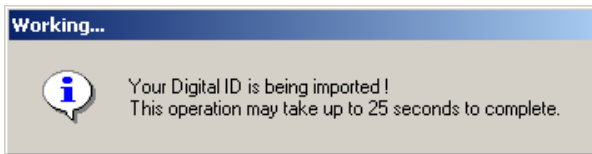


Figure 31: Import Digital ID: Working

→ Your Digital ID is being imported

6

When the Digital ID has been successfully imported, the following prompt will inform you:

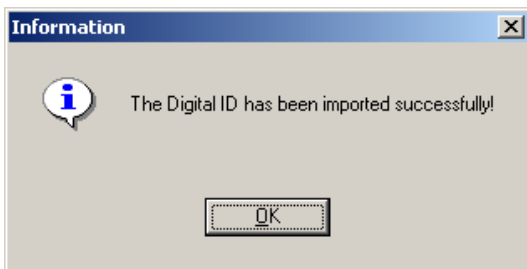


Figure 32: Import Digital ID: The Digital ID has been imported successfully

→ Click **OK** to close this dialog



Key Size Error

When you try to import a Digital ID that does not comply with the key length constraints of the supported tokens, the following dialog will be displayed:

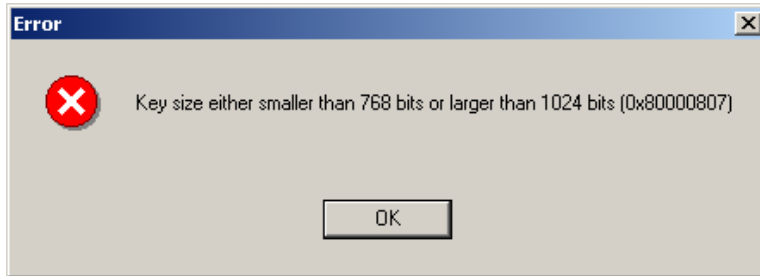


Figure 33: Error: Key Size either smaller than 768 bits or larger than 1024 bits

Click **OK** to close this dialog



Token out of Memory

When the token is full, i.e. does not have enough memory to import a / another Digital ID, the following dialog will be displayed:



Figure 34: Error: Token out of memory

Click **OK** to close this dialog.

You may check in the *Token Information* dialog (**Token > Show Token Info**) how much space is left on the token. Note that the token may contain parts of the Digital ID file imported (e.g. when it contains multiple certificates).

For more information on the SafeSign Token Management Utility, see the *SafeSign Token Management Utility Guide / Token Administration Guide*.

3.3 Generate a Digital ID using Check Point VPN-1 SecuRemote / SecureClient GUI

This paragraph will describe how to create a Check Point certificate (issued by the Check Point Internal CA) directly on the SafeSign token, using the Check Point VPN-1 SecuRemote / SecureClient application.

For this user guide, the VPN-1 SecuRemote application has been used.

Note that in order to perform this procedure; a user should have been created on the server, for which a certificate has been initiated (including a registration key) that is pending to be requested.

On the client machine, in the Check Point VPN-1 SecuRemote application, select **Certificates > Check Point Certificates > Create** to request a Check Point certificate:

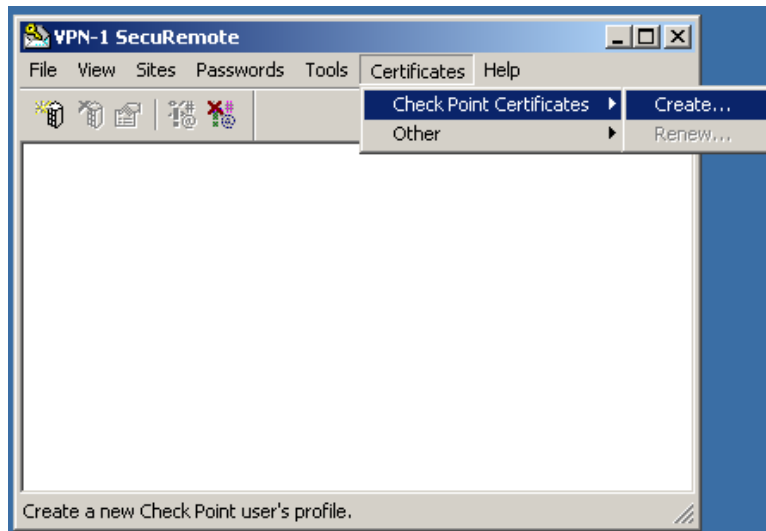


Figure 35: VPN-1 SecuRemote: Create Check Point Certificate

The first *Check Point Certificate* dialog will enable you to select the desired certificate storage type:

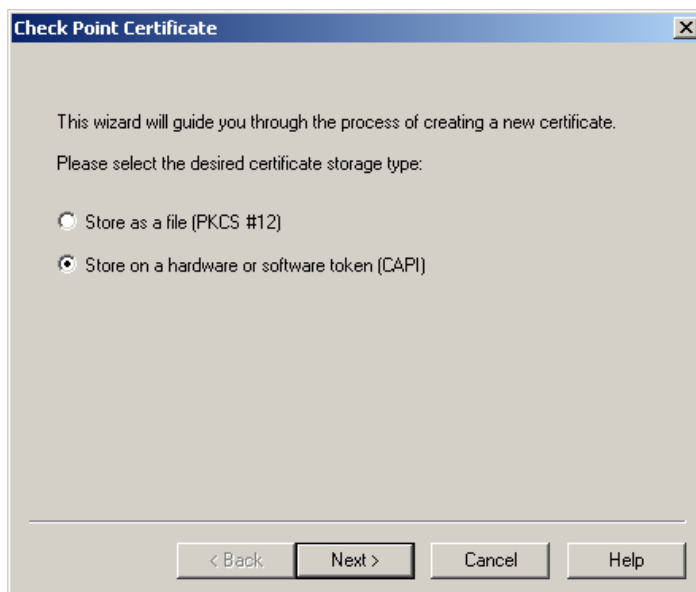


Figure 36: Check Point Certificate: certificate storage type

➔ Select the option "Store on a hardware or software token (CAPI)" as above and click **Next**

The next dialog will allow you to select the Cryptographic Service Provider for the certificate storage:

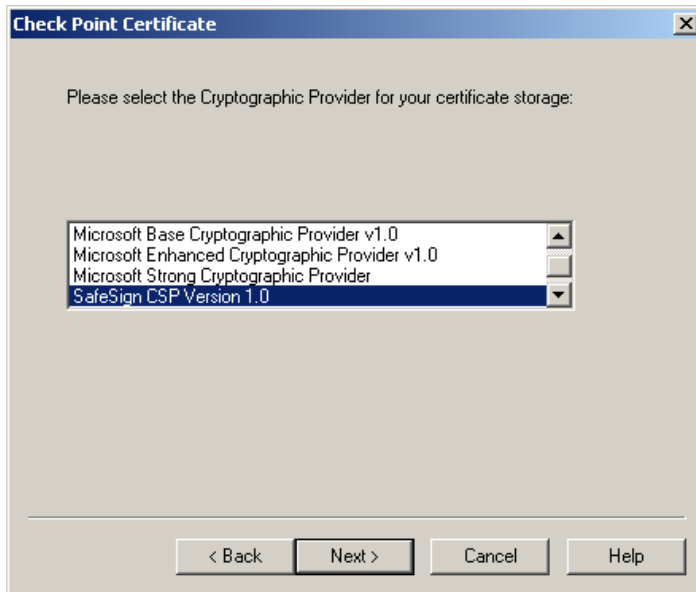


Figure 37: Check Point Certificate: Cryptographic Provider

➔ Select the "SafeSign CSP Version 1.0" (as above) and click **Next**

After selecting the cryptographic provider for the certificate storage, you will be asked to enter the Certificate Authority IP address or name and the Registration key:

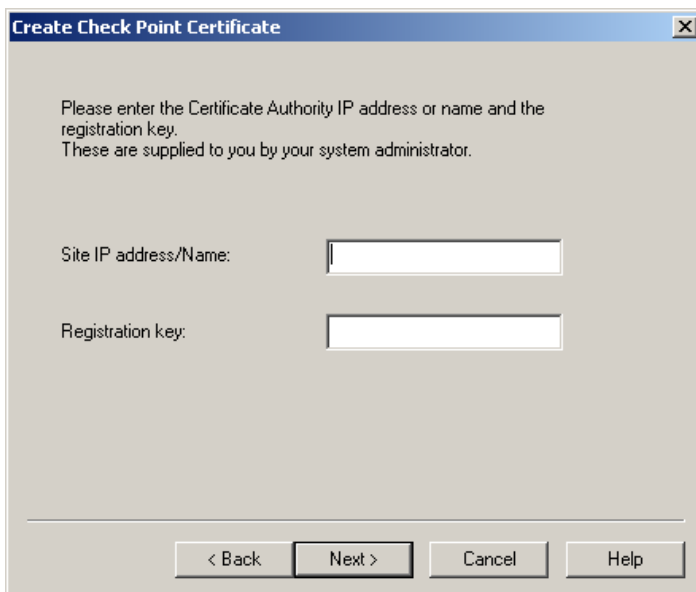


Figure 38: Create Check Point Certificate: Site address and registration key

➔ Enter the site's IP address/Name and the registration key provided to you

During the process of retrieving your certificate, you will be asked to enter the PIN for your SafeSign token:

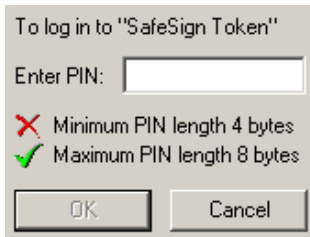


Figure 39: SafeSign Login

➔ Enter the PIN for your SafeSign token and click **OK**



Root Certificate Store

You may also be asked if you want to add to add the certificate to the root certificate store:



Figure 40: Root Certificate Store

➔ Click **OK** to add the certificate to the root store

When the certificate has been created successfully, the final dialog will appear:

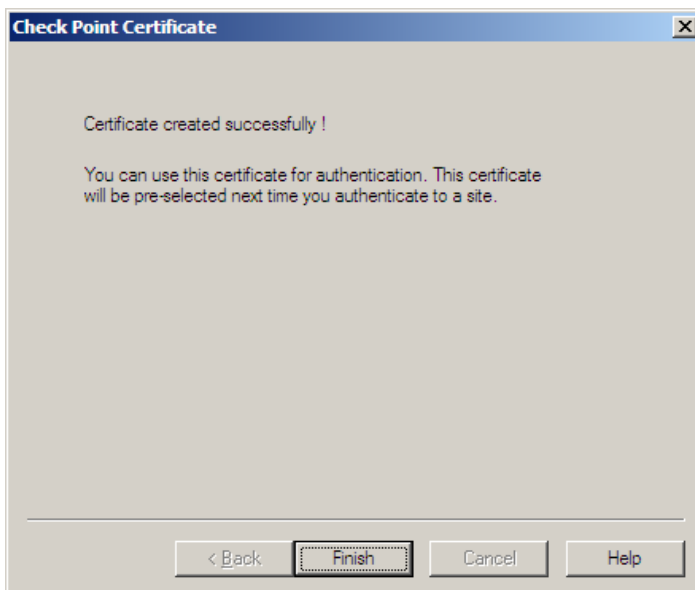


Figure 41: Check Point Certificate: Certificate created successfully

➔ Click **Finish**

You can now use this certificate to log on to your Check Point VPN-1 / FireWall-1 Gateway.

3.4 Generating a Digital ID issued by Microsoft CA

This paragraph will describe how to request a certificate through a web browser from an OPSEC certified Certificate Authority.

For instructions on how to configure the Check Point VPN-1 / FireWall-1 for OPSEC PKI, see [Chapter 4](#).

For this user guide, the Microsoft CA was used. Note that the steps described below provide an example of such procedure for Windows CA only.

Open a browser (in this example Microsoft Internet Explorer) and access the site of the Microsoft certificate authority:

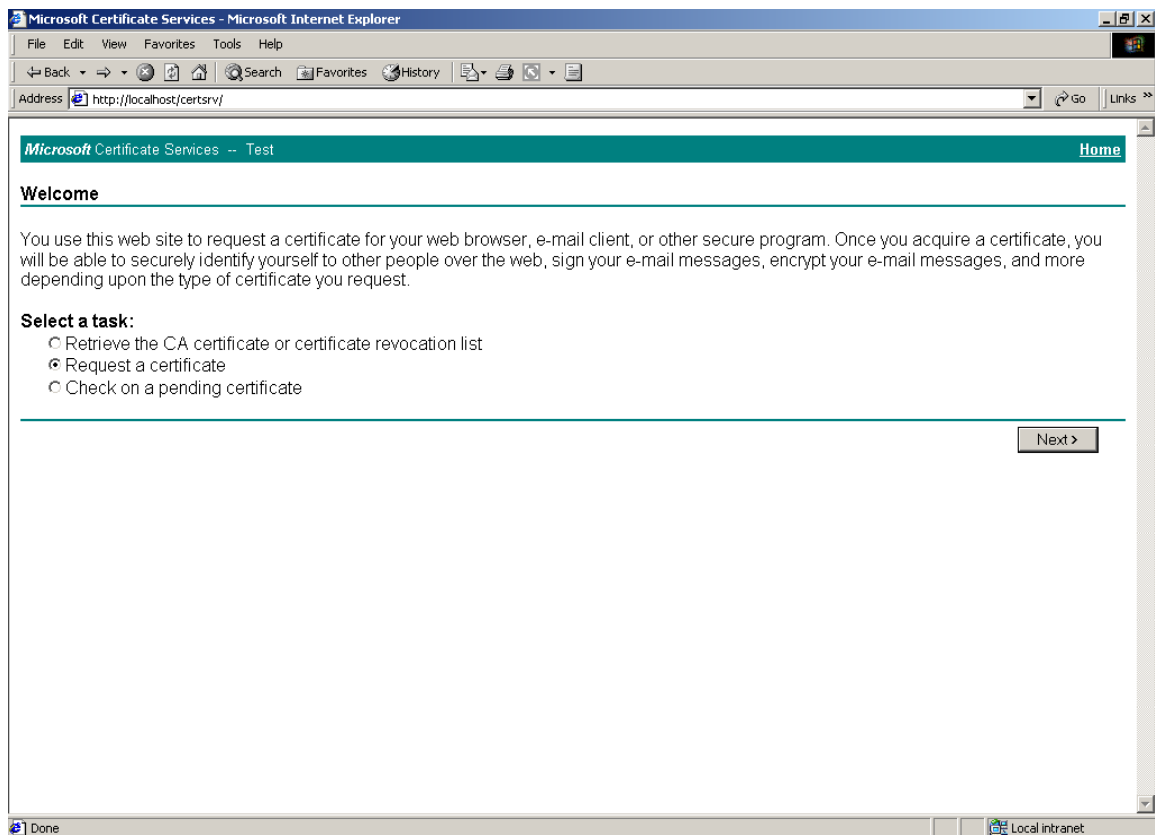


Figure 42: Microsoft certificate Services: Request a certificate

➔ Select "Request a certificate" (as above) and click **Next**

Upon clicking **Next**, the *Choose Request Type* window will open:

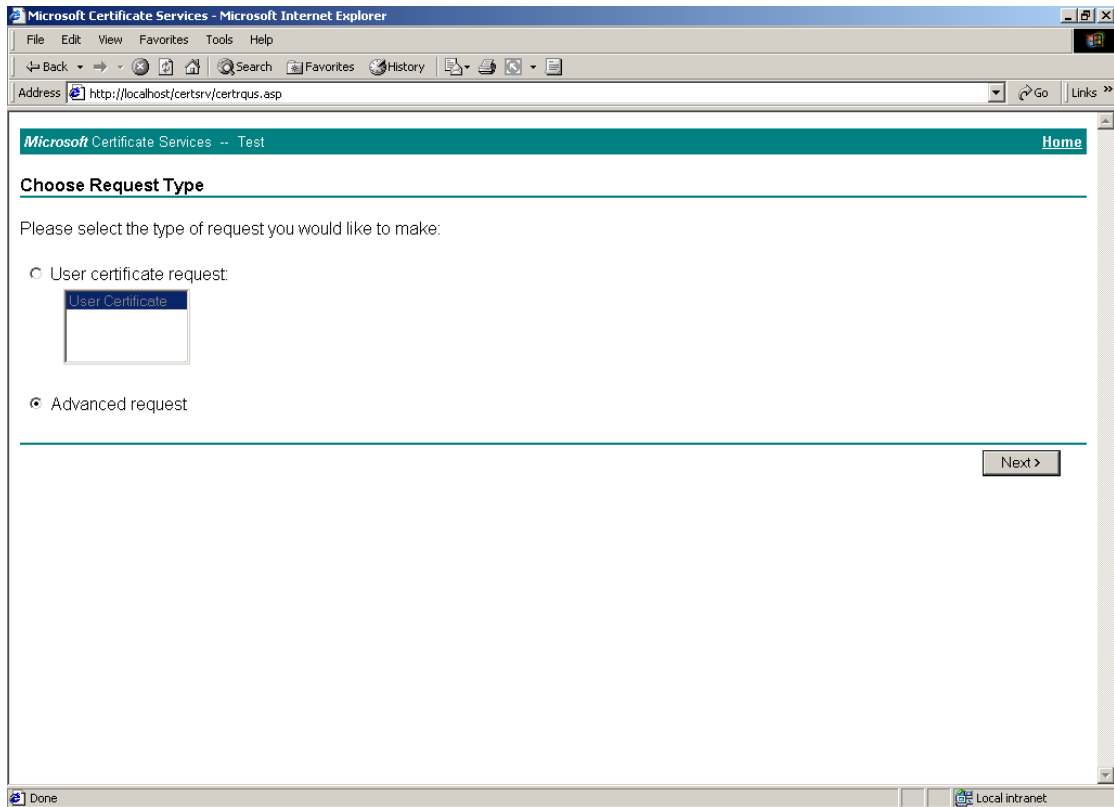


Figure 43: Microsoft Certificate Services: Choose Request Type

➔ Select "Advanced Request" (as above) and click **Next**

Upon clicking **Next**, the *Advanced Certificate Requests* window will open:

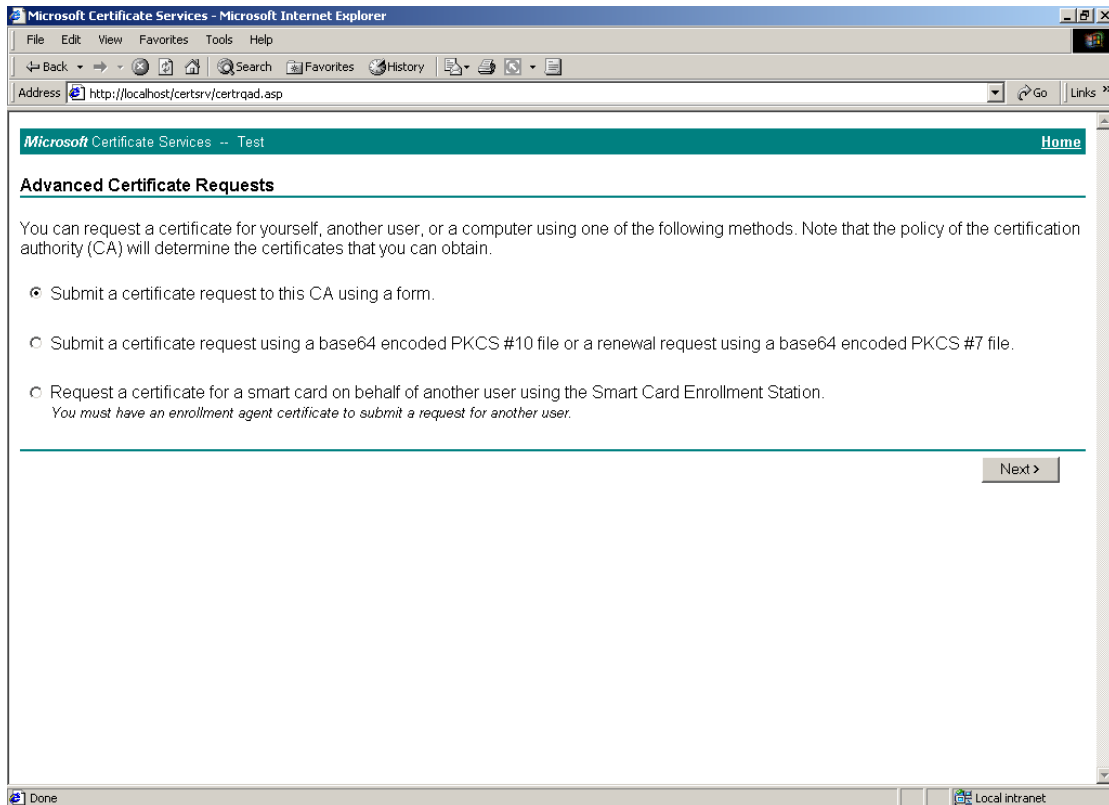


Figure 44: Microsoft Certificate Services: Advanced Certificate Requests

➔ Select “Submit a certificate request to this CA using a form” and click **Next** to continue

The next dialog will allow you to set some options for your certificate request:

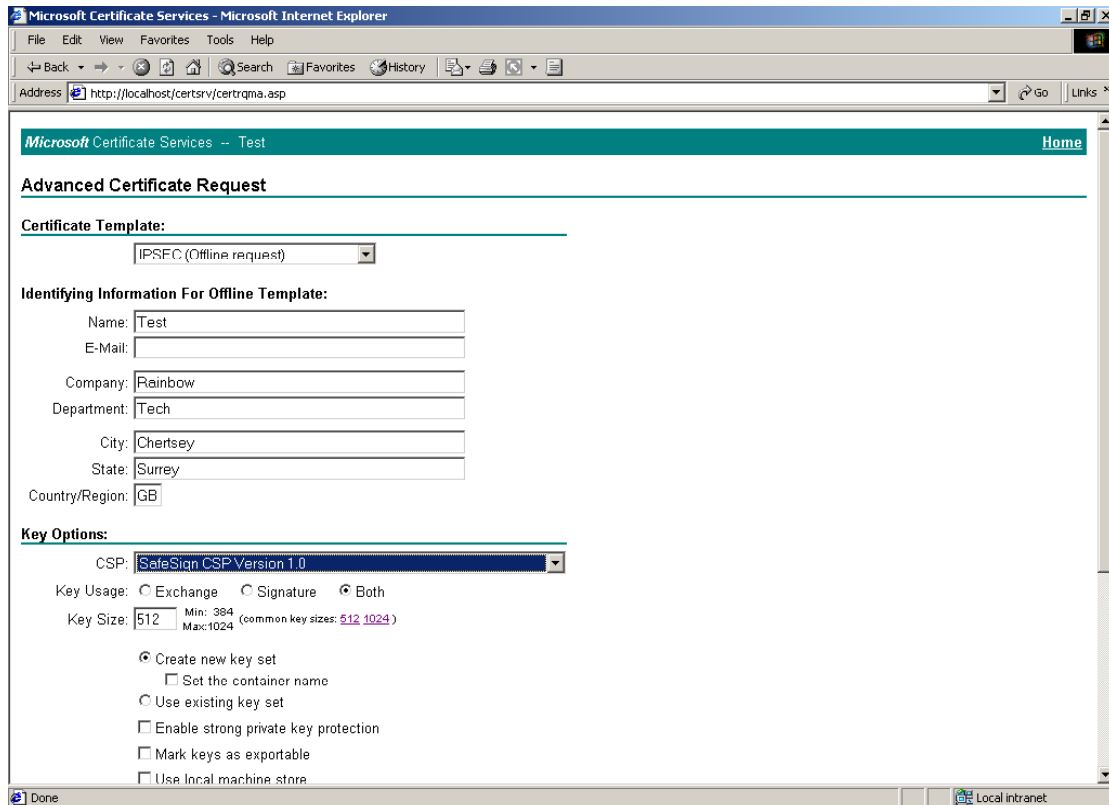


Figure 45: Microsoft Certificate Services: Certificate options

- ➔ Do the following:
- ➔ Select "IPSEC (Offline request)" from the dropdown menu under Certificate template;
- ➔ Enter the user name (as created in the VPN-1 / FireWall-1 server);
- ➔ Select "Safesign CSP Version 1.0" as the CSP, with 1024 as your key size
- ➔ Then click **Submit** to generate the key pair.

You will be asked to enter the PIN for your SafeSign token:

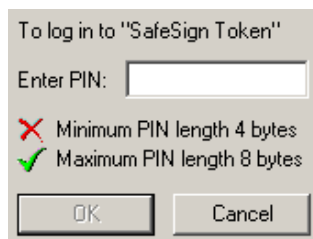


Figure 46: SafeSign Login

- ➔ Enter the PIN for your SafeSign token and click **OK**

Wait for the server's response, until you are allowed to install the certificate:

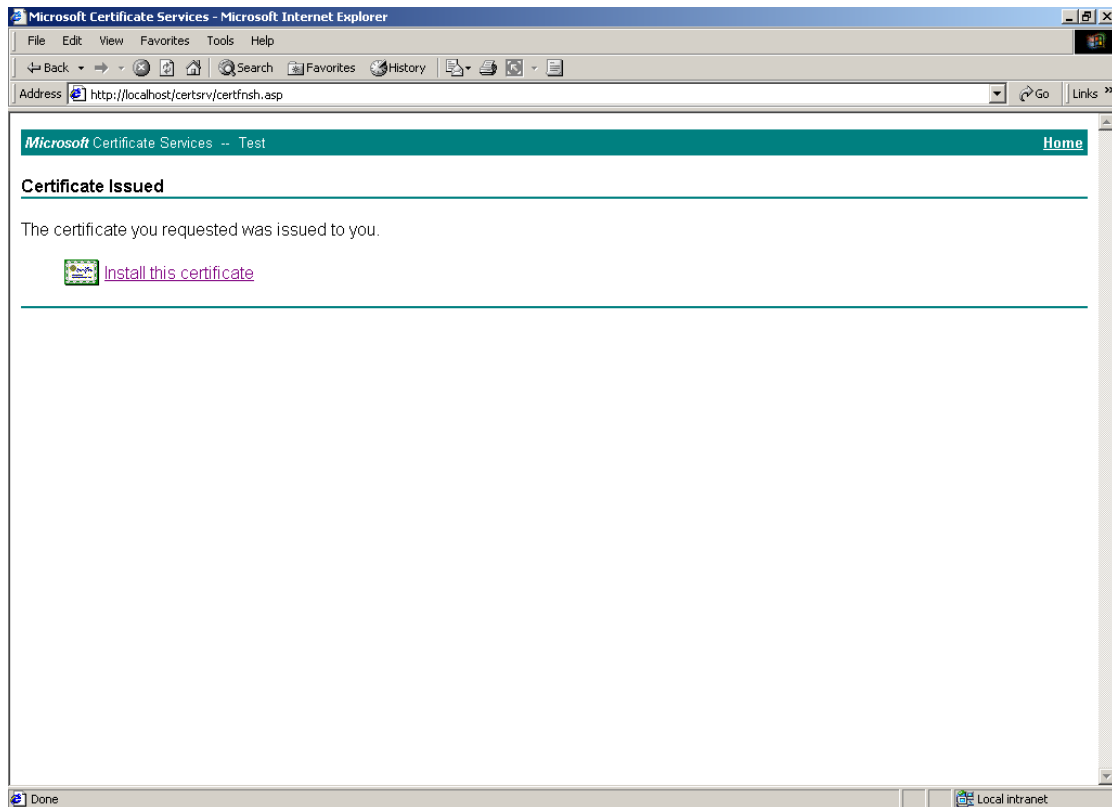


Figure 47: Microsoft Certificate Services: Certificate issued

- ➔ Click on [install this certificate](#), whereupon the certificate will be installed both on the host and on the SafeSign token.

When the certificate is installed, you will be informed:

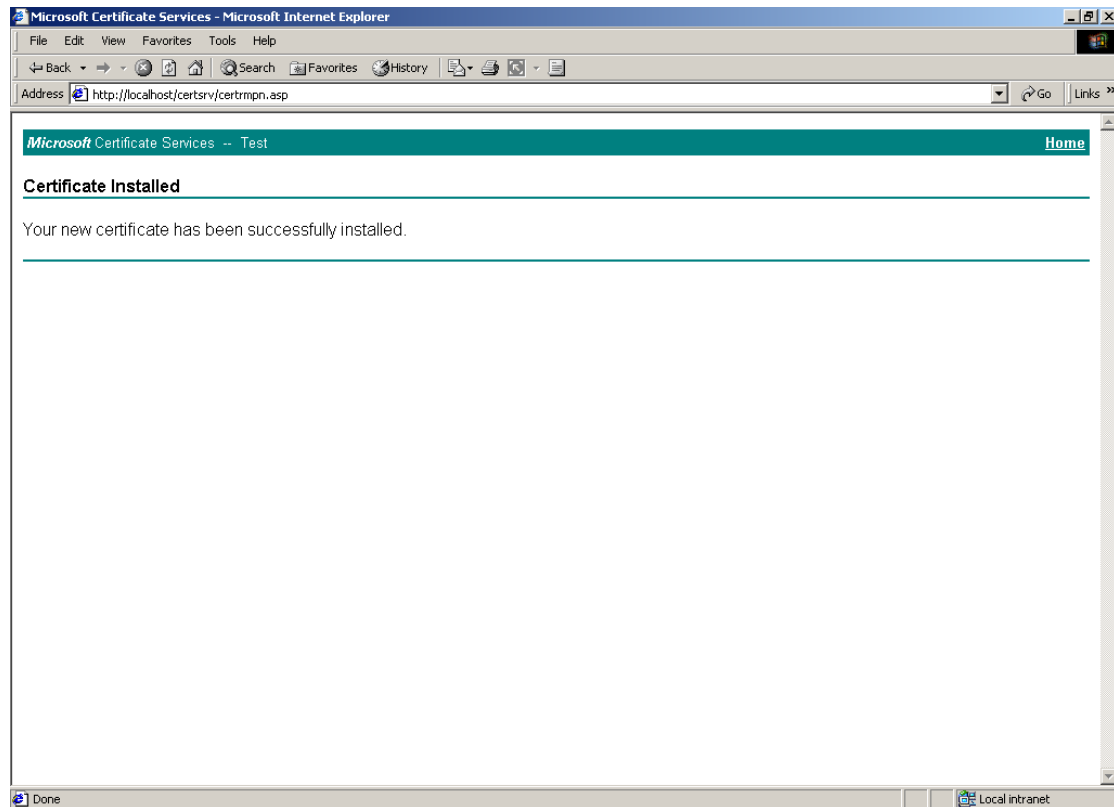


Figure 48: Microsoft Certificate Services: Certificate installed

➔ You can now close the browser

Your token is now ready with a certificate to be used to log on to VPN-1/ FireWall-1 Gateway using the Check Point VPN-1 SecuRemote / SecureClient application.

See [paragraph 2.2](#) for instructions on how to create a site.

4 Setting up Checkpoint NG FP3 VPN-1 / FireWall-1

This chapter deals with how to configure Checkpoint VPN-1 / FireWall-1 NG FP3 to use the Microsoft CA to authenticate users. In order to do, you should follow a number of steps, described in the next paragraphs.

[Obtain the CA certificate](#)

[Create CA Server](#)

[Generate a PKCS#10 certificate request](#)

[Request a Windows 2000 IPSEC certificate](#)

[Install IPSEC certificate for the Gateway](#)

[Configure IKE](#)

[Create new user](#)

The steps and screenshots below have been made using a Check Point NG FP3 VPN-1 / FireWall-1. The configuration described was used for OPSEC certification testing. If you are using a different version, the configuration steps are likely to be different.

4.1 Obtain the CA certificate



Note

To create this manual, Microsoft Enterprise CA was used, but you may also use the Microsoft Standalone CA.

The first step in configuring your OPSEC PKI, is to obtain the CA certificate of the Windows Enterprise CA.

In your browser, go to the site of the Microsoft certificate authority to open the following window:

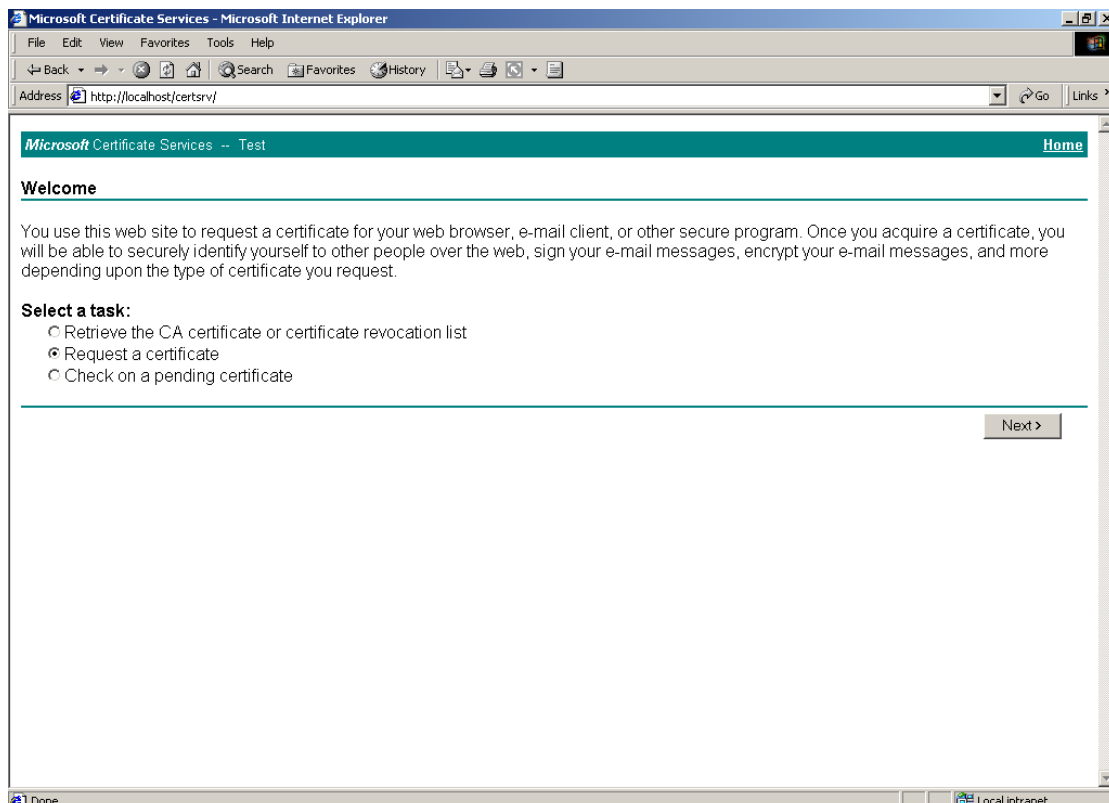


Figure 49: Microsoft Certificate Services: Welcome page CA

➔ Select “Retrieve the CA certificate or certificate revocation list” and click **Next**

Upon clicking **Next**, the *Retrieve The CA Certificate or Certificate Revocation List* window allows you to download the CA certificate:

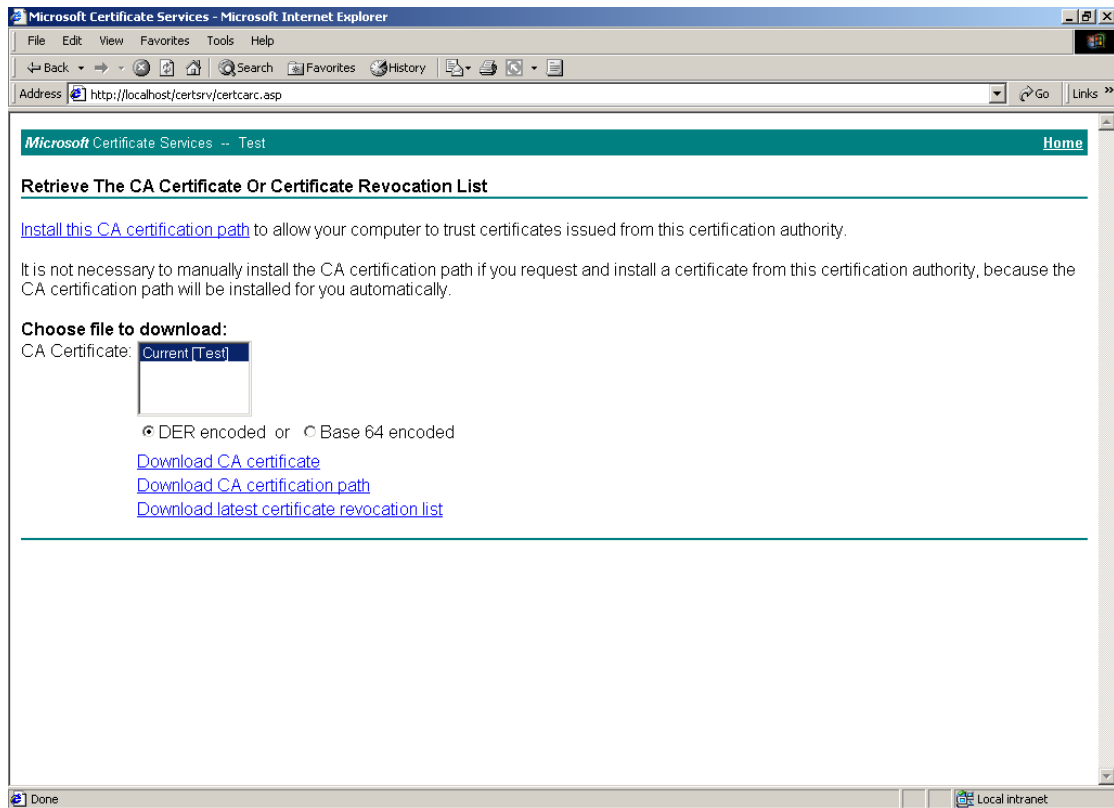


Figure 50: Microsoft Certificate Services: Retrieve the CA Certificate

➔ Make sure "DER encoded" is selected and click on [Download CA certificate](#)

When prompted to open the file or save the file to disk, select **Save this file to disk** (as below):

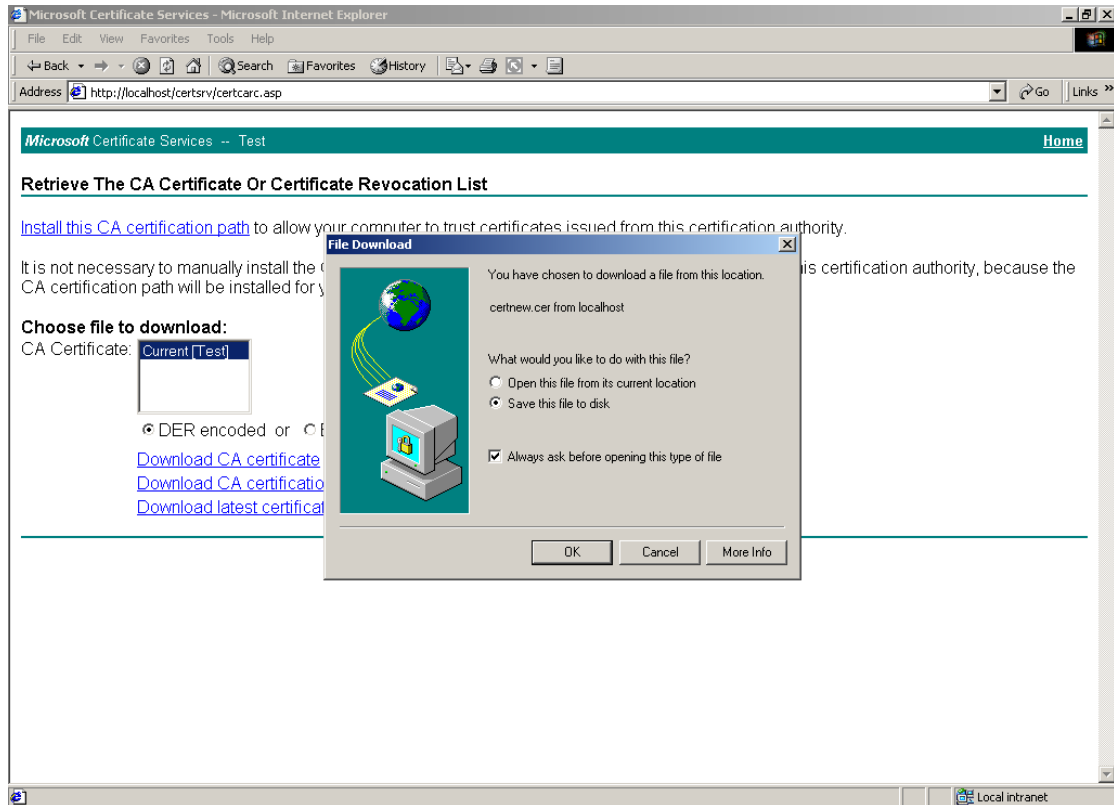


Figure 51: Microsoft Certificate Services: Save this file to disk

➔ Save the file into a path and when the file is saved, close the *File Download* dialog (if required)

Now that you have downloaded the CA certificate, you will need to create this (Microsoft) CA server in Check Point VPN-1 / FireWall-1 and install the (above) downloaded CA certificate for the Gateway.

Note: You will also need to install this CA certificate on your client machine.

4.2 Create CA Server

The second step is to create the Microsoft CA server in Check Point VPN-1 / FireWall-1 and install the CA certificate via the SmartDashboard.

Run SmartDashboard NG FP3 from:

Start > Programs > Check Point SMART Clients > SmartDashboard NG FP3

Enter your password to login and when logged in, go to **Manage > Servers** to open the *Servers* dialog:

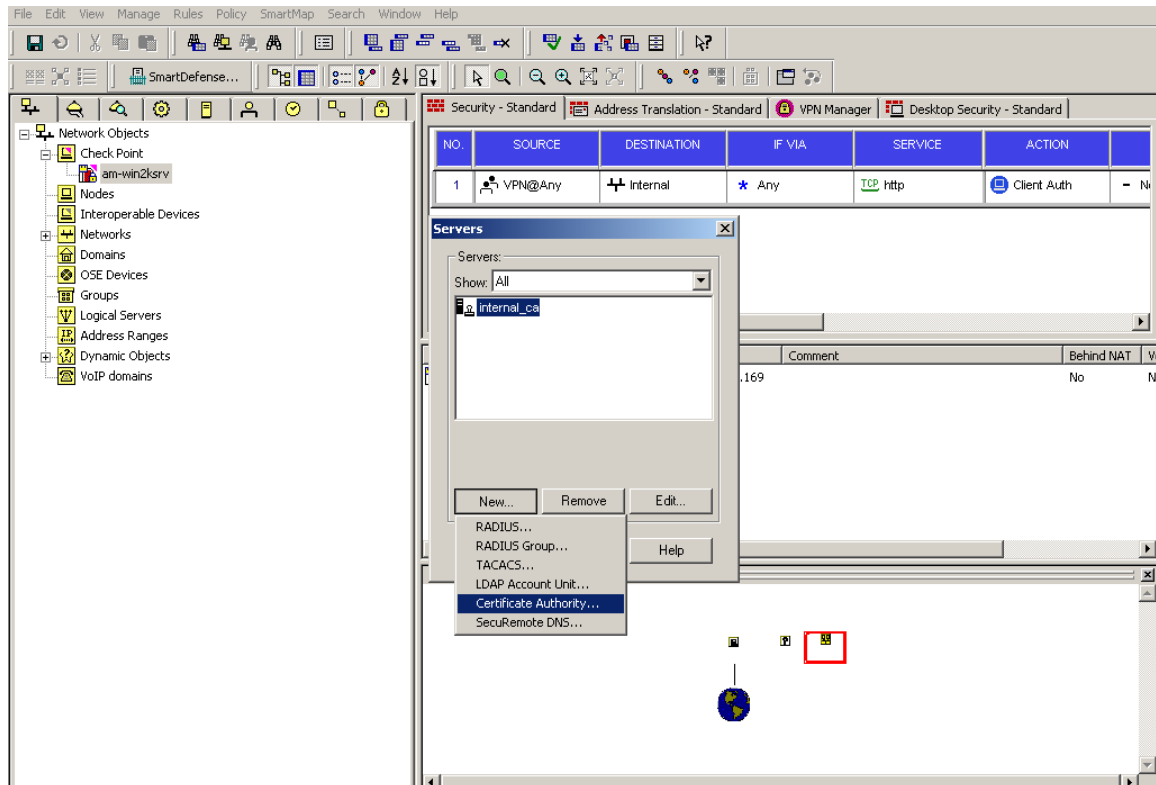


Figure 52: SmartDashboard: New Certificate Authority

➔ Click on **New** in the *Servers* dialog (as above) and then select **Certificate Authority**

This will open the Certificate Authority Properties dialog:

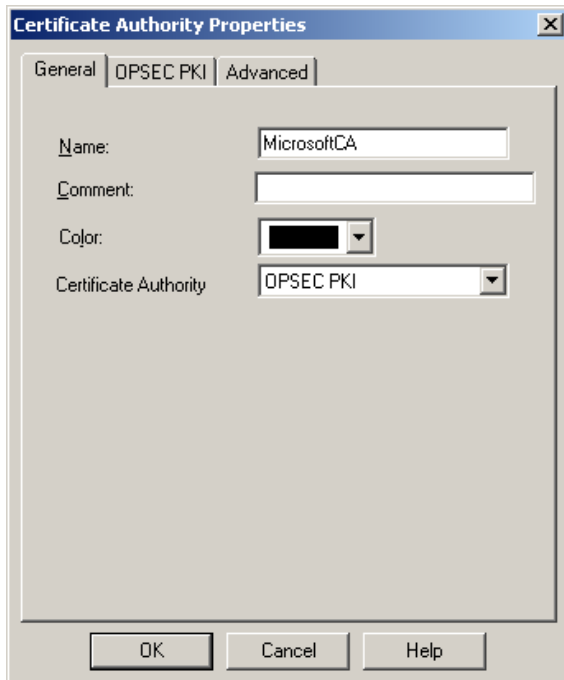


Figure 53: Certificate Authority Properties: General tab

➔ In the *General* tab, enter the name of your CA and select OPSEC PKI (as above)

Next, select the *OPSEC PKI* tab and make sure the 'HTTP Server(s)' option is ticked:

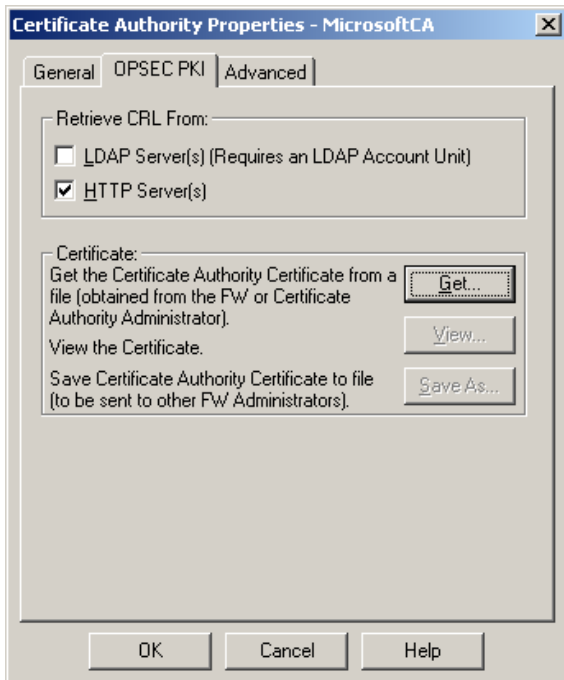


Figure 54: Certificate Authority Properties: OPSEC PKI tab

➔ Click on **Get** to get the Certificate Authority Certificate from a file

Select the CA certificate file that you have downloaded when obtaining the Microsoft CA certificate (as described in [paragraph 4.1](#)):

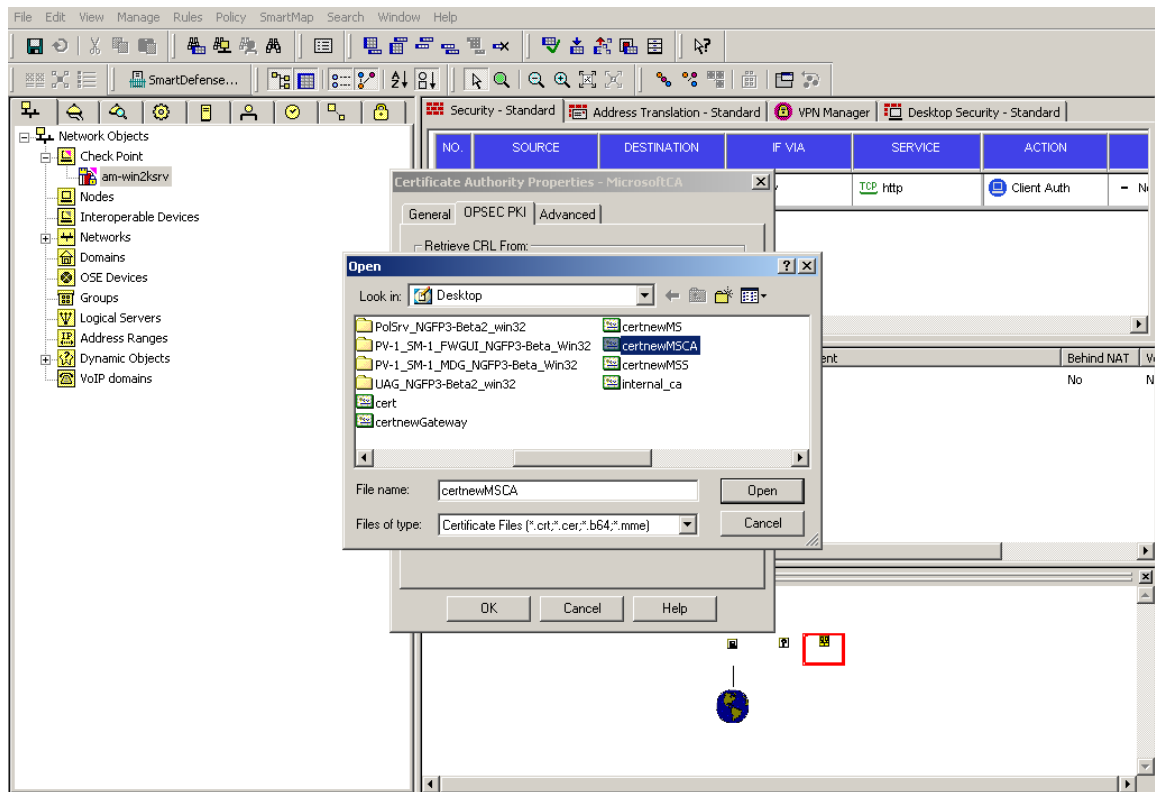


Figure 55: SmartDashboard: Get Certificate Authority Certificate

- ➔ Click **Open** (as above) and when asked in the *Certificate Authority Certificate View* dialog “Do you accept this Certificate Authority certificate?” select **OK**.
- ➔ Then click **OK** to close the *Certificate Authority Properties – MicrosoftCA* dialog.

Your newly created CA is now displayed in the list in the *Servers* dialog:

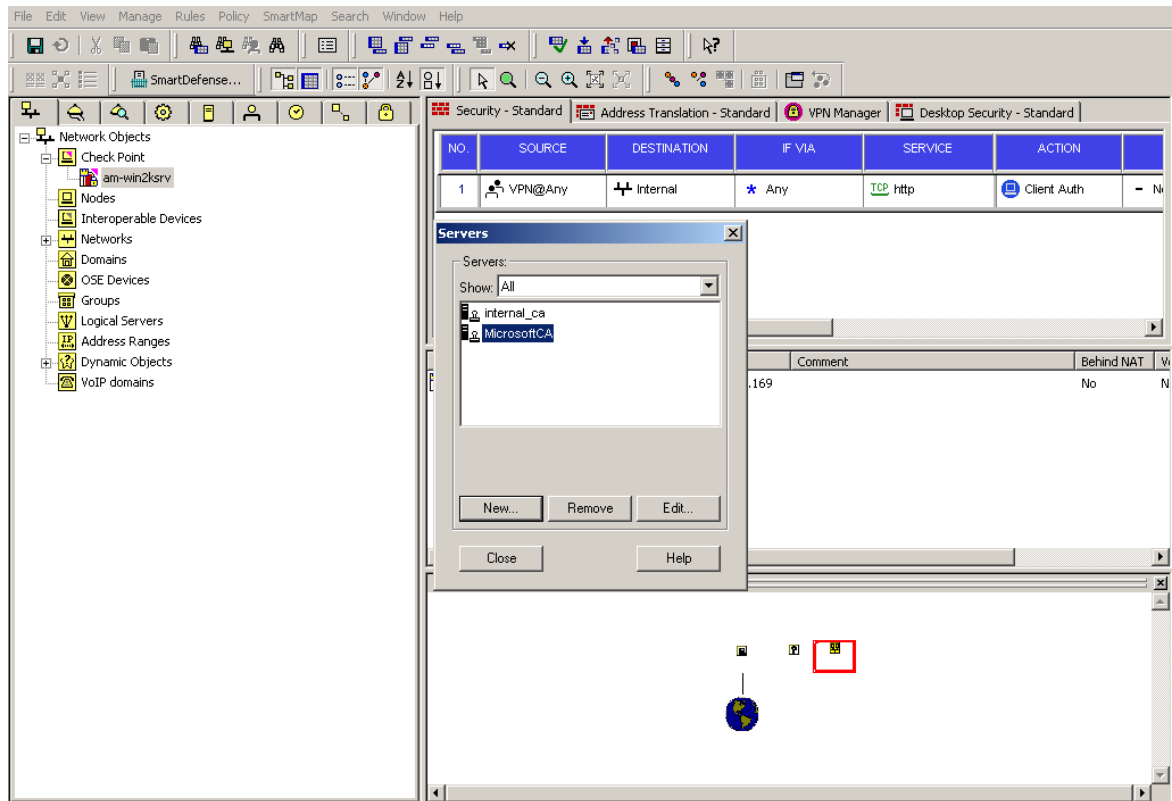


Figure 56: SmartDashboard: Microsoft CA Server created

➔ Click **Close** to close the *Servers* dialog

Now you will need to generate a PKCS#10 Certificate request for the Gateway (assuming that there is an already created Gateway workstation for which the CA will generate a certificate).

4.3 Generate a PKCS#10 Certificate Request

The third step is to generate a PKCS#10 certificate request for the Gateway.

Select **Manage > Network Objects** to open the *Network Objects* dialog:

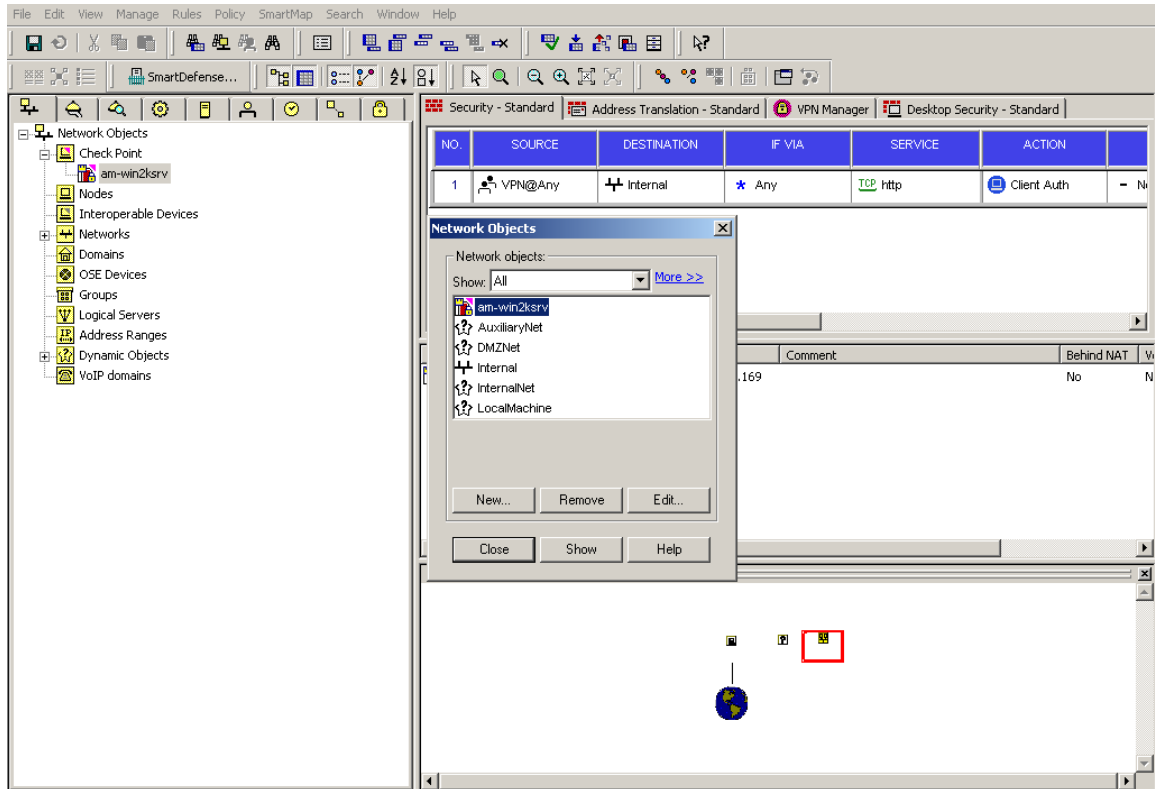


Figure 57: SmartDashboard: Network Objects

➔ Select your previously created workstation (as above) and click **Edit**

This will open the *Check Point Gateway* dialog for the Gateway workstation you selected for editing. Select the VPN tab (as below):

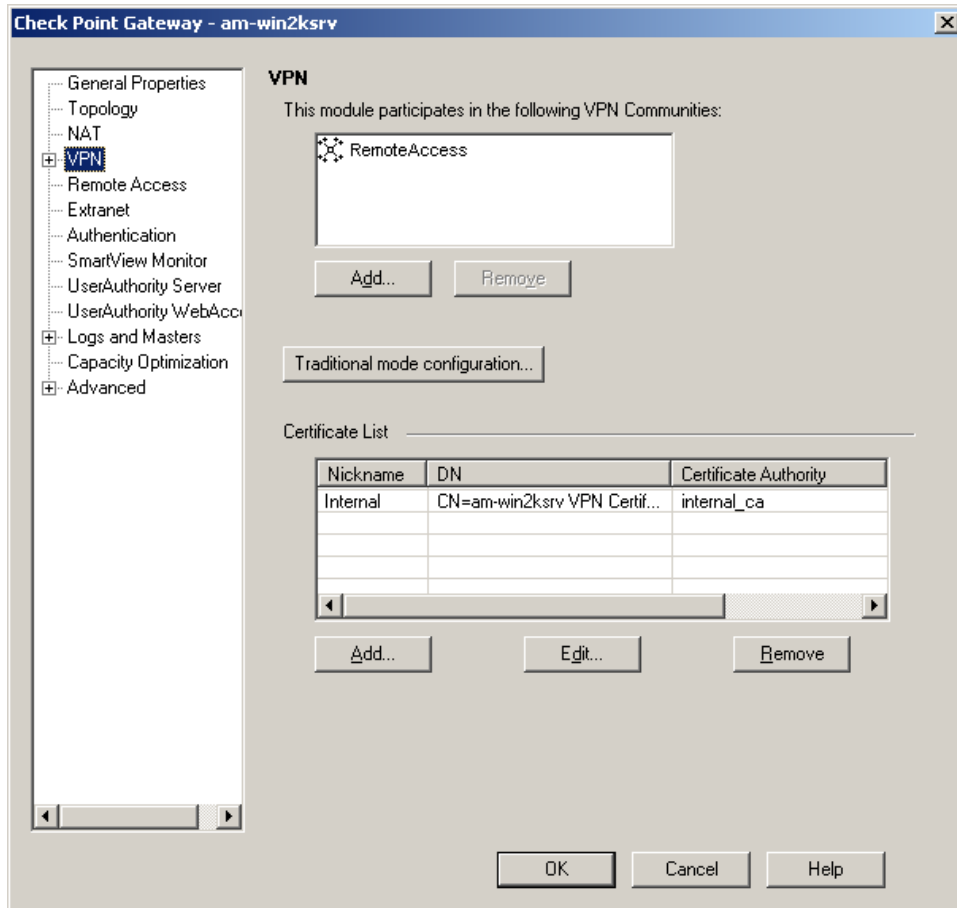


Figure 58: Check Point Gateway: VPN

➔ In the Certificate List section, click **Add**

Enter a Certificate Nickname (MicrosoftCA in our example) and select the previously created and defined CA server ('MicrosoftCA') from the Certificate Authority dropdown list as below:

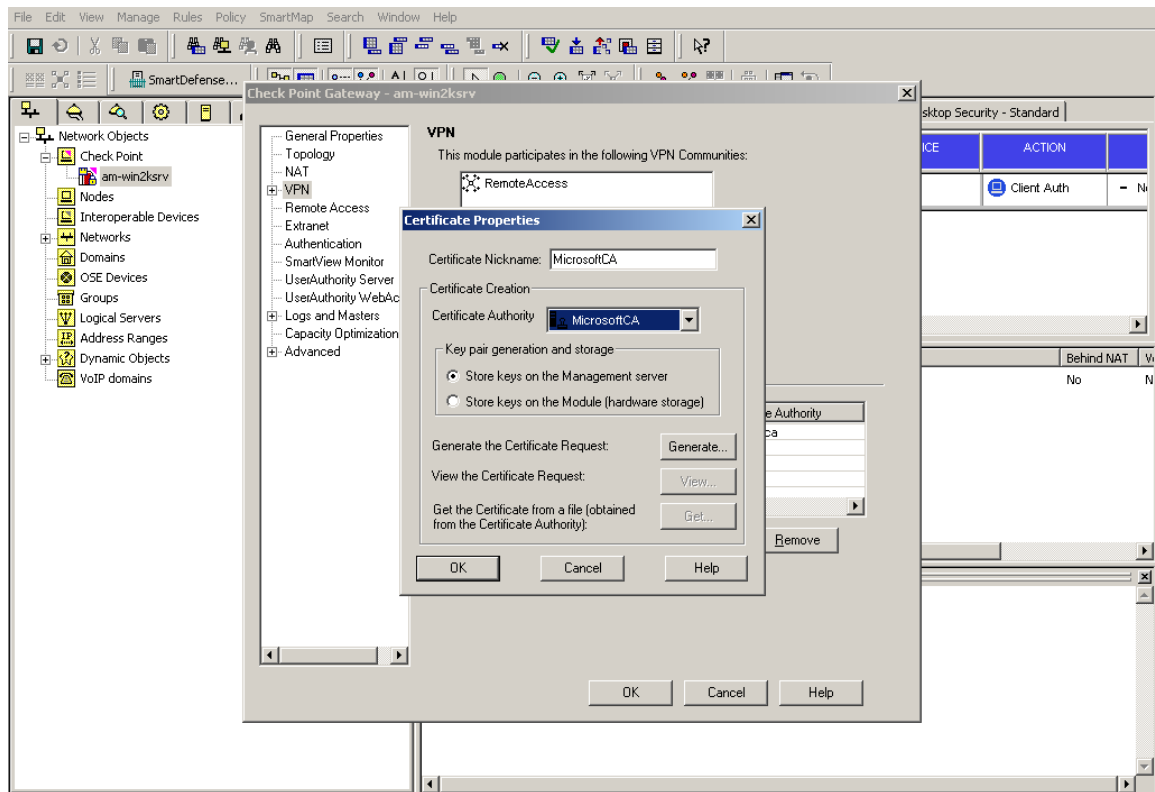


Figure 59: Check Point Gateway: Certificate Properties

➔ Click on **Generate** to generate the PKCS#10 certificate request

At the prompt “The generation of the certificate for the node cannot be undone, unless you click Remove. Are you sure you want to continue?” click **Yes** and enter the Distinguished Name for the Gateway in the DN field:

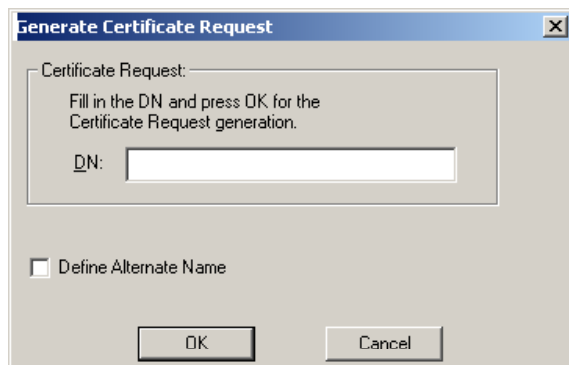


Figure 60: Generate Certificate Request

➔ Click **OK**

When the Generate Certificate Request was successful, you will be informed that the certificate request was created successfully:

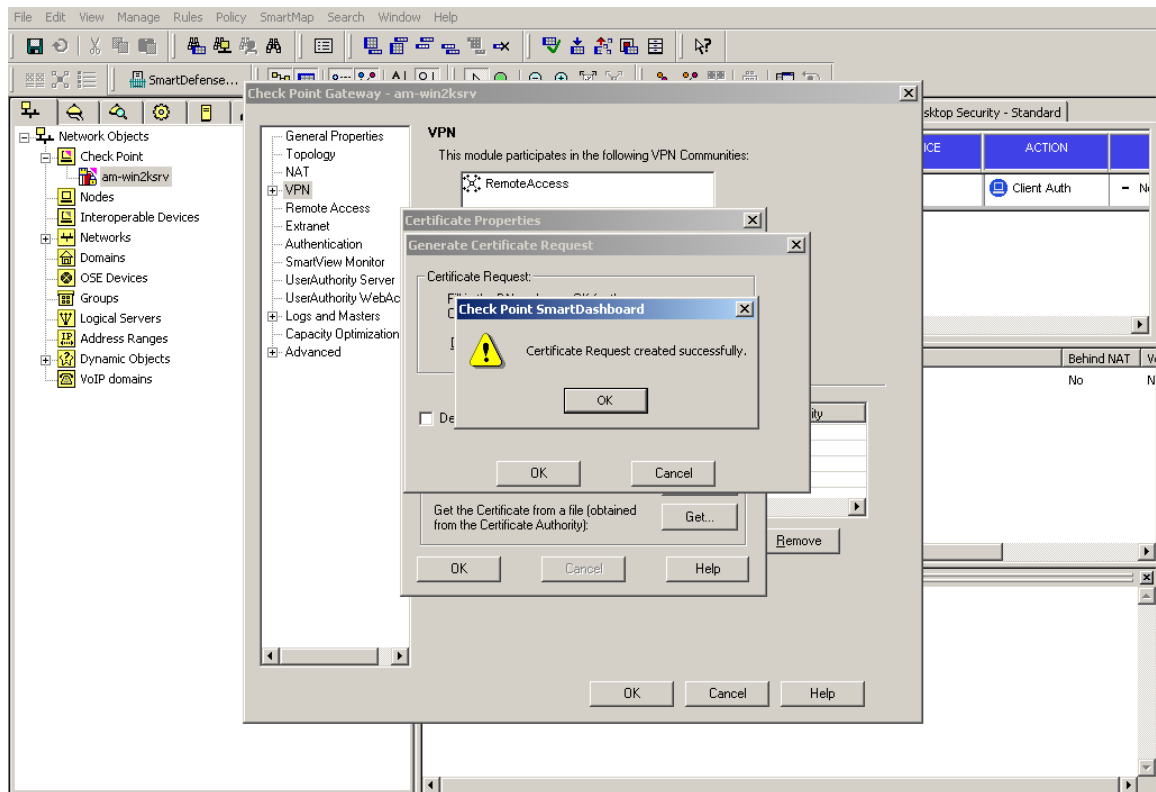


Figure 61: Generate Certificate Request successful

➔ Click **OK**

Upon clicking **OK**, you will return to the *Certificate Properties* dialog:

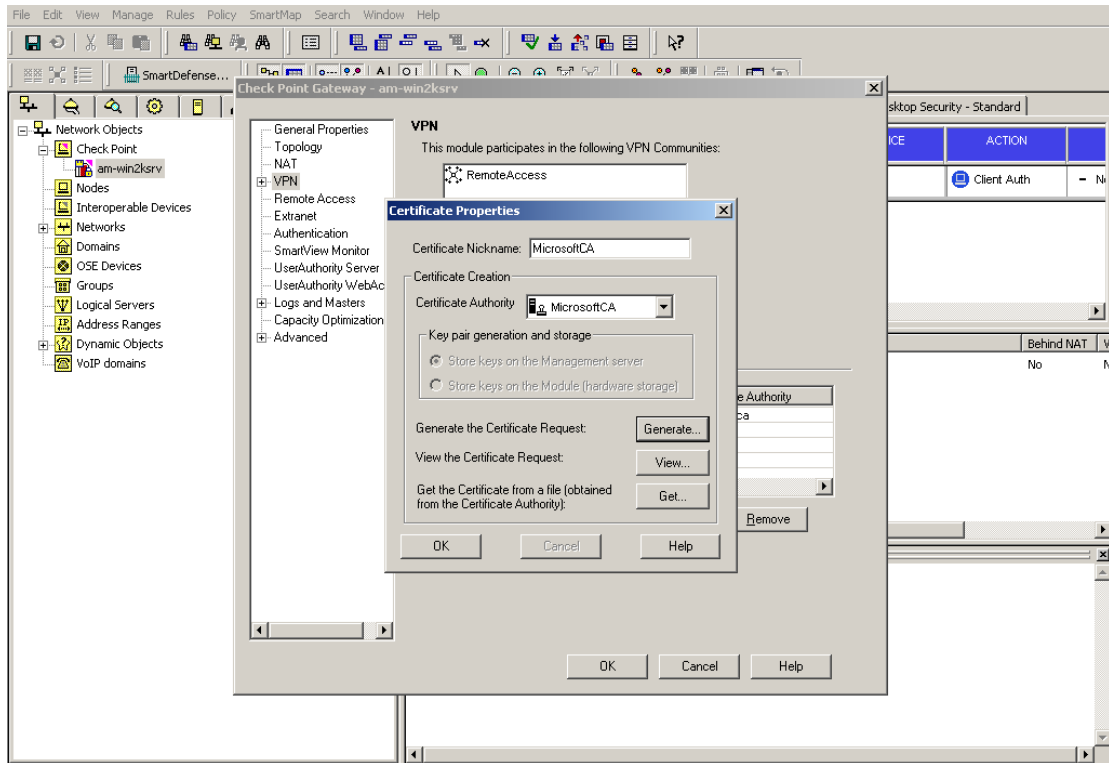


Figure 62: Check Point Gateway: Certificate Properties

➔ Click **View** to view the certificate request

After clicking **View**, select and copy the contents of the *Certificate Request View* dialog (i.e. the PKCS #10 Certificate request text) into the clipboard:

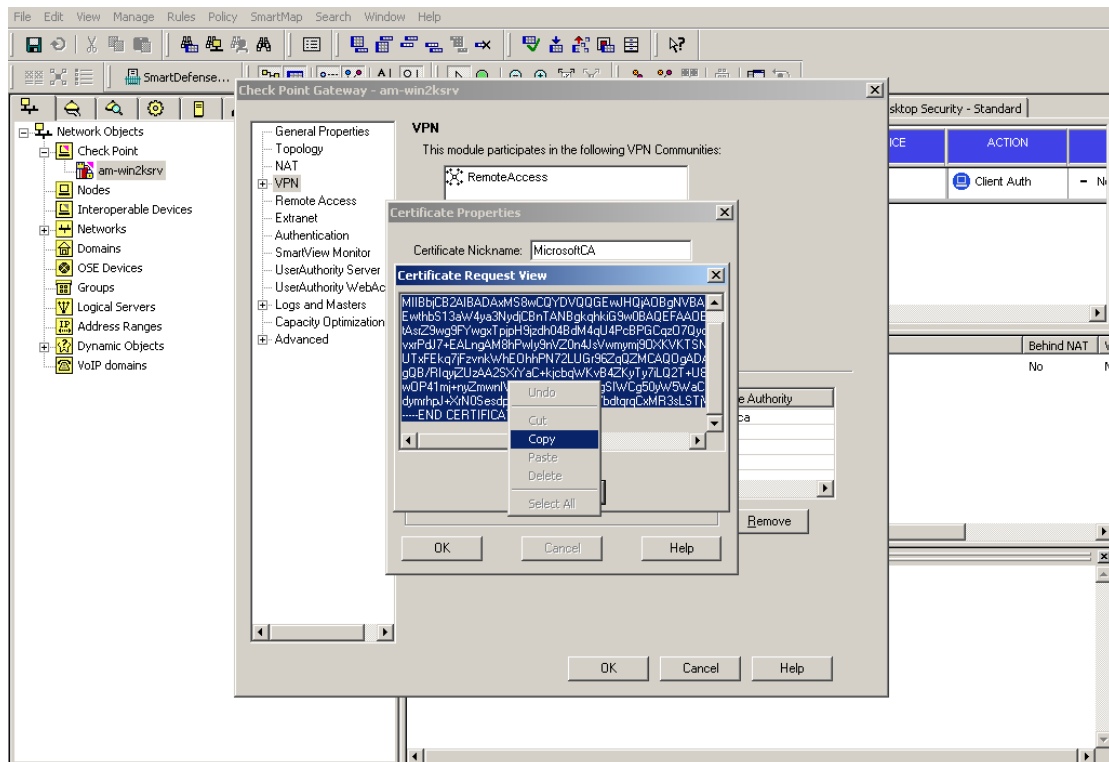


Figure 63: Certificate Request View

This text should be used for the next step, when you request a windows 2000 IPSEC certificate for the Gateway ([paragraph 4.4](#)).

Note that you may also copy this content into a text file for convenience.

➔ Click **OK**, close all the windows and save the Policy.

Now you will need to request a windows 2000 IPSEC certificate for the Gateway.

4.4 Request a Windows 2000 IPSEC certificate

The fourth step is to request a Windows 2000 IPSEC certificate for the Gateway.

Open up a browser and go to the URL of your Certificate Authority:

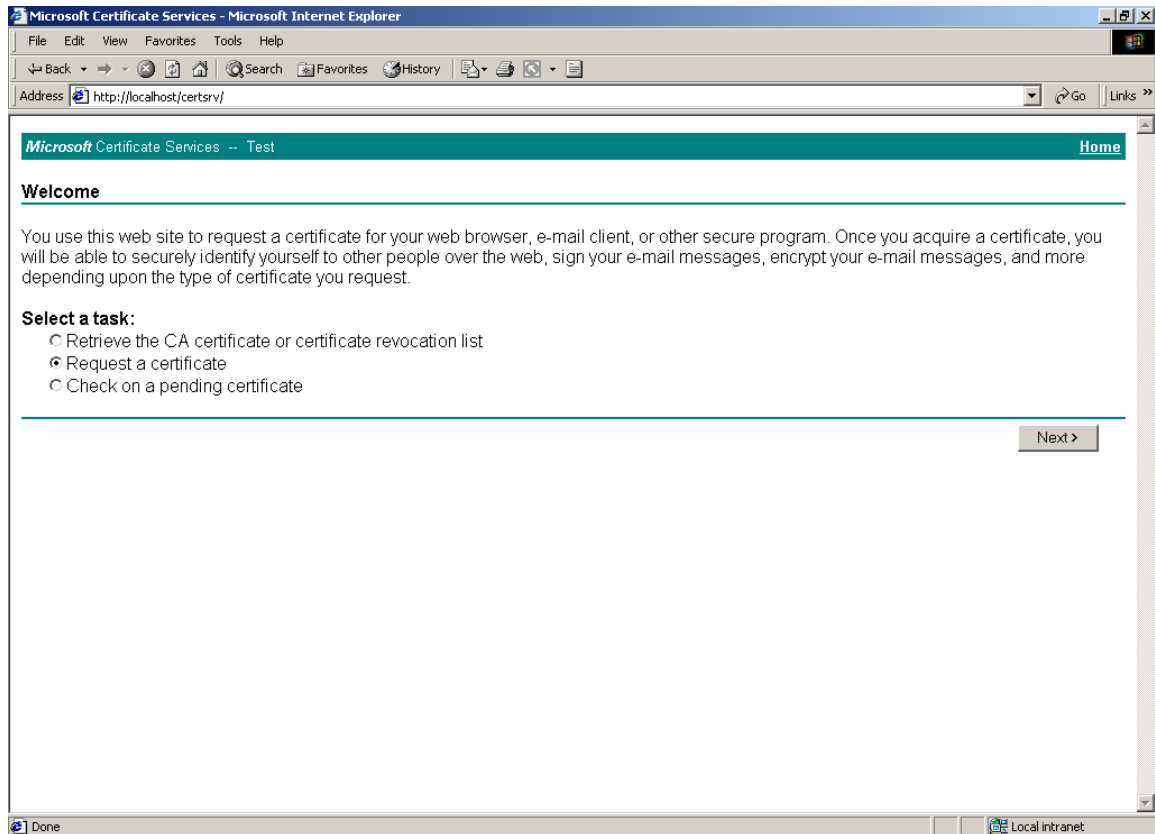


Figure 64: Microsoft Certificate Services: Request a certificate

➔ Select “Request a certificate” and click **Next**

In the *Choose Request Type* window, select “Advanced request” (as below):

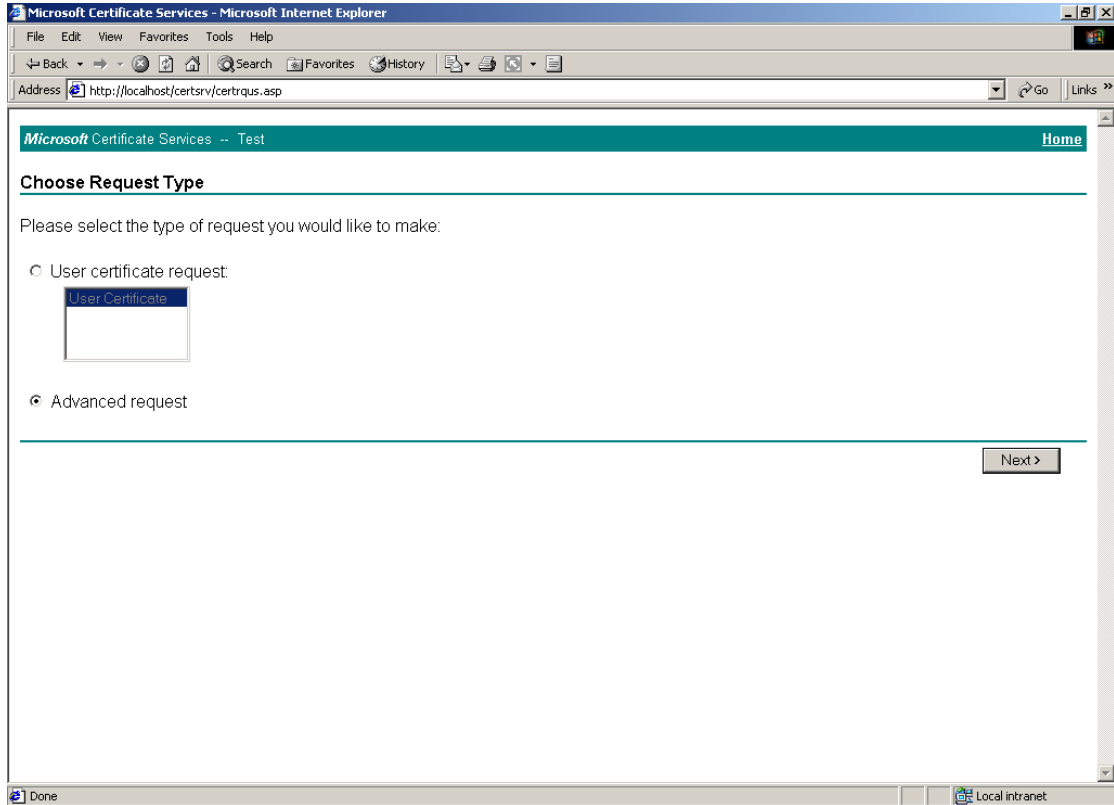


Figure 65: Microsoft Certificate Services: Choose Request Type

➔ Click **Next**

In the *Advanced Certificate Requests* window, select “Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS#7 file” (as below):

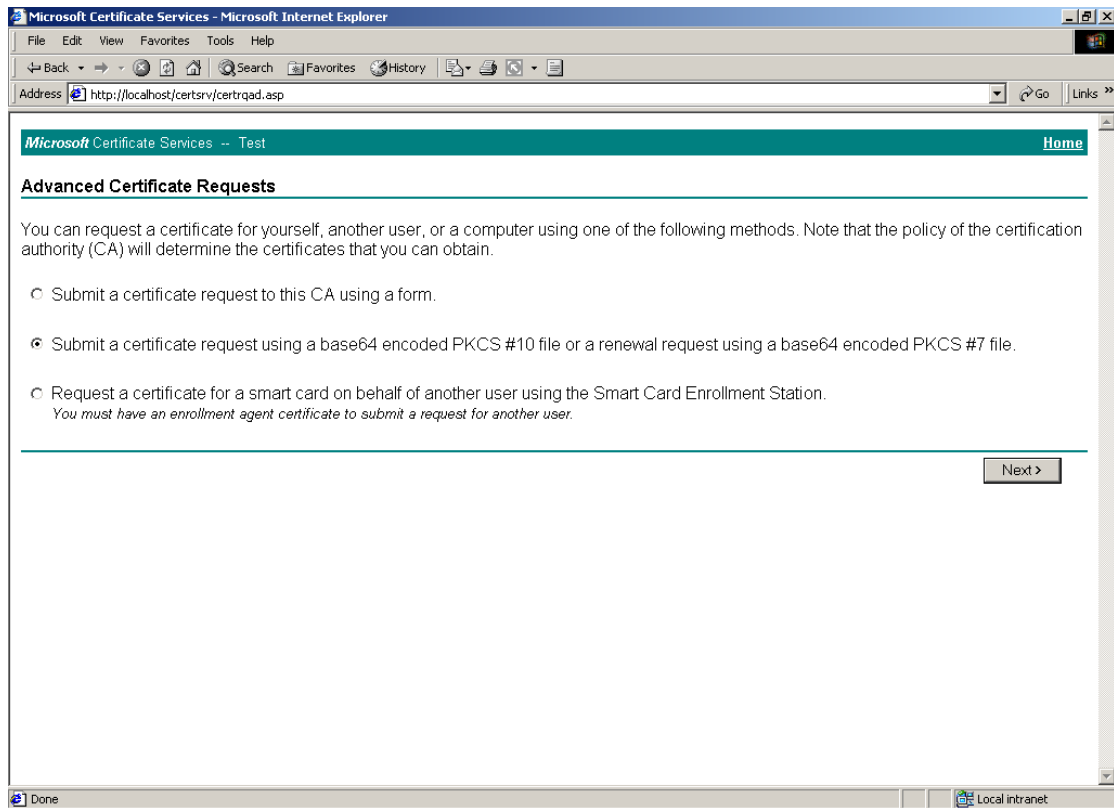


Figure 66” Microsoft Certificate Request: PKCS#10 request

➔ Click **Next**

Paste the content of your PKCS #10 certificate request text (as copied in [Figure 63](#)) into the *Saved Request* field (as below):

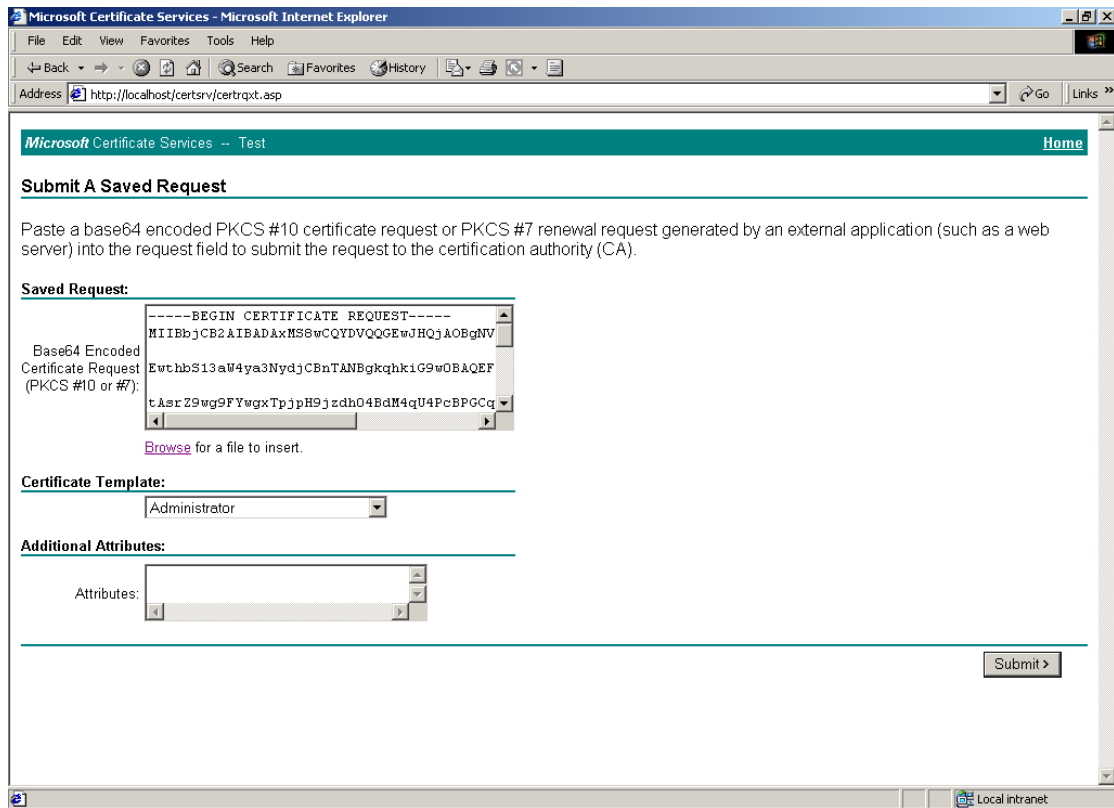


Figure 67: Microsoft Certificate Services: Saved request

➔ Click **Submit**

If the Microsoft CA is configured to issue certificates immediately, the following window will be displayed:

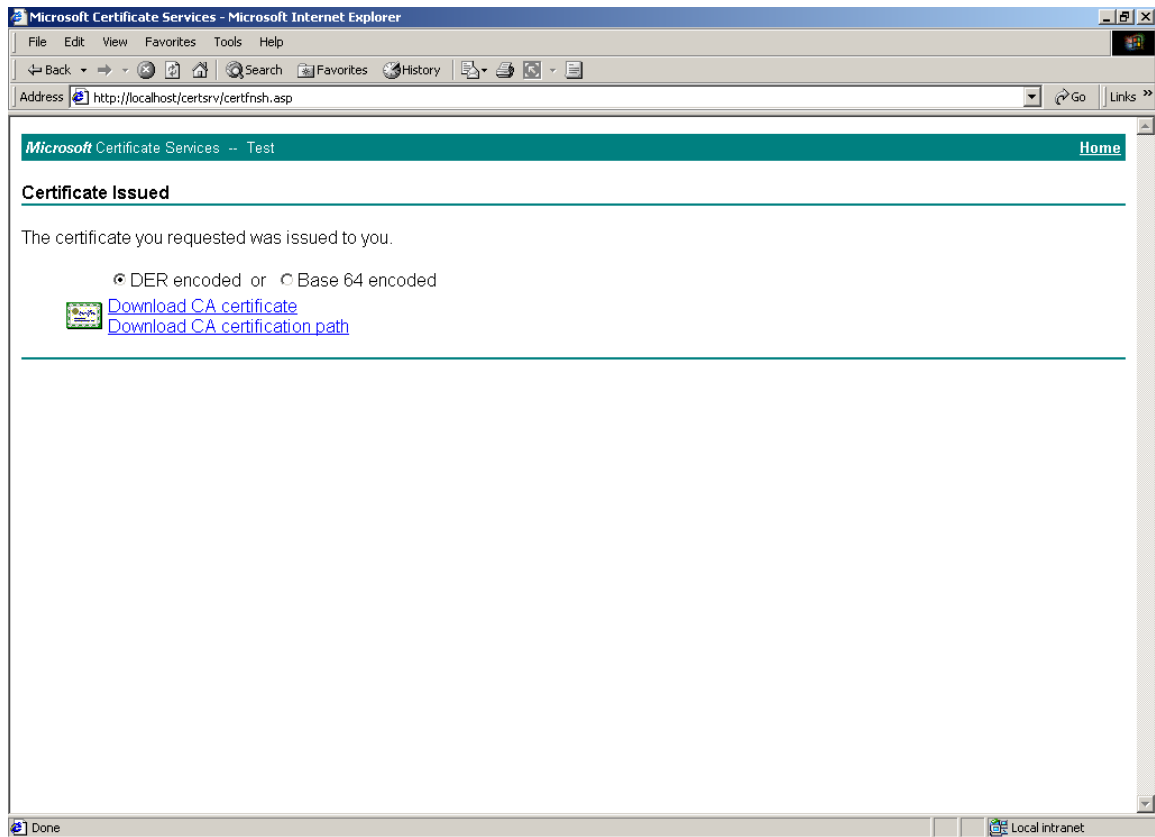


Figure 68: Microsoft Certificate Services: Download CA certificate

➔ Click **Download CA certificate** and save the file into a desired path on your machine.

Now that you have downloaded the Windows 2000 IPSEC certificate for the Gateway, you are ready to install it in the Check Point VPN-1 / FireWall-1 for your Gateway.

4.5 Install IPSEC certificate for the Gateway

The fifth step is to install the Windows 2000 IPSEC certificate you have downloaded in the previous step in the Check Point VPN-1 / FireWall-1 for your Gateway.

Start the Check Point SmartDashboard as described before ([paragraph 4.2](#)).

When logged in, go to Manage > Network Objects

Select your previously created Gateway workstation and click on **Edit**

After clicking on **Edit**, select the VPN tab to open the following window:

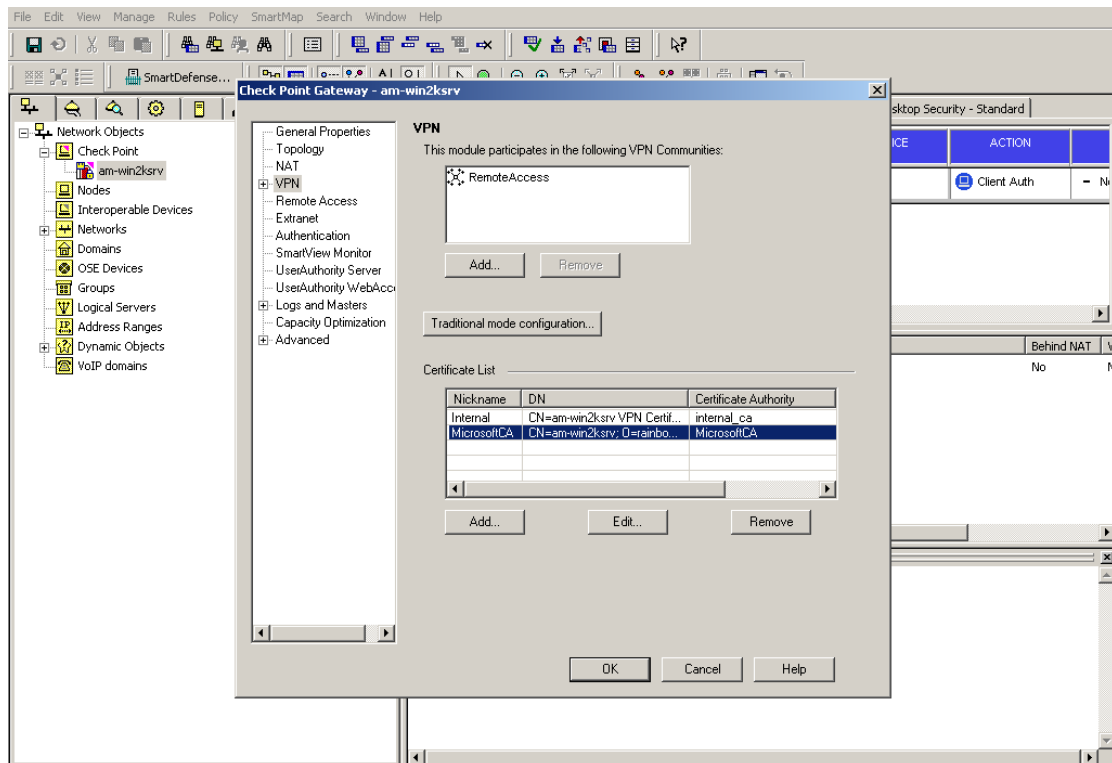


Figure 69: SmartDashboard: VPN

➔ Select your previously created Microsoft CA (as above) and click on **Edit**

Clicking on **Edit** will open the *Certificate Properties* dialog:

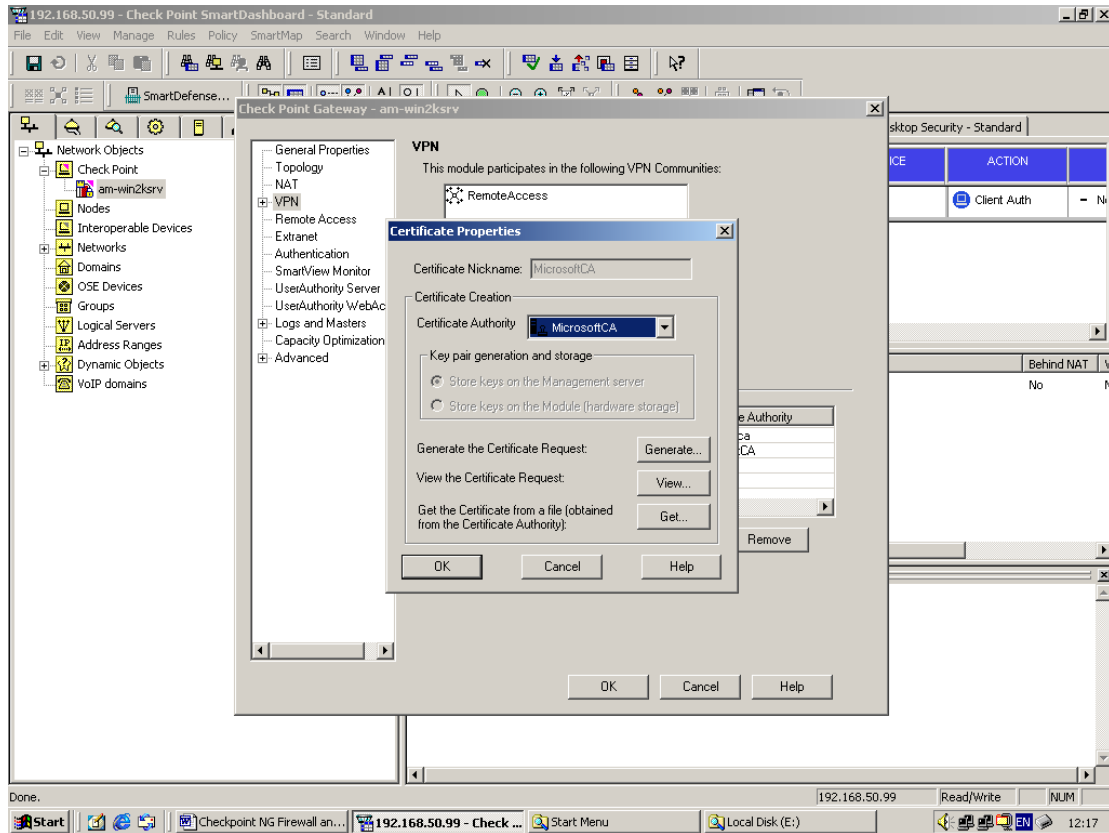


Figure 70: SmartDashboard: Certificate Properties

- ➔ Click on **Get** to get the certificate from a file (obtained from the Certificate Authority) and select the Gateway certificate you have just downloaded ([Figure 68](#)) from your Microsoft CA.
- ➔ Click **OK** when prompted by the *Certificate View* dialog: "Do you accept this Certificate?"
- ➔ Close all other windows and Save your policy.

Now you have to configure IKE in the Check Point VPN-1 / FireWall-1.

4.6 Configure IKE

The sixth step is to configure IKE in Check Point VPN-1 / FireWall-1.

In the Check Point SmartDashboard, go to **Manage > Network Objects**

Select your Gateway workstation and click on **Edit**

After clicking on **Edit**, select the **Topology** tab:

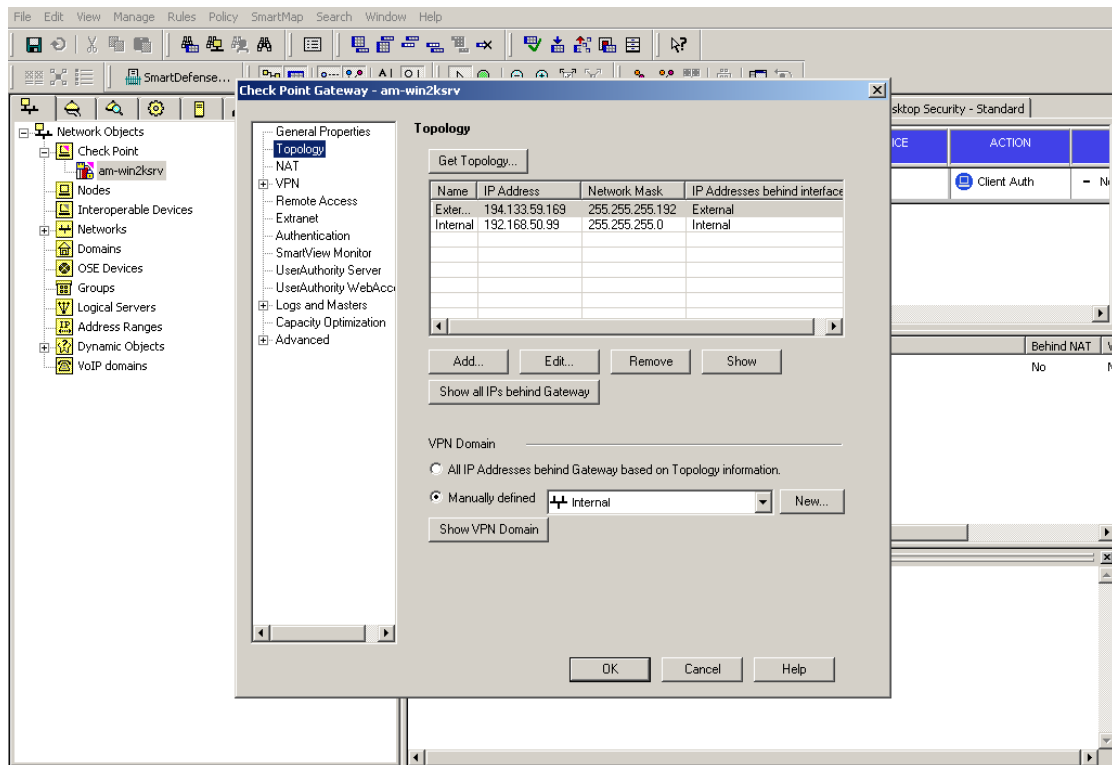


Figure 71: SmartDashboard: Topology

- ➔ Select **Manually defined** in the VPN Domain area and select the group/network that the Gateway will encrypt, from the dropdown list

Next, select the VPN tab (Figure 69) and click **Traditional mode configuration** to open the following window:

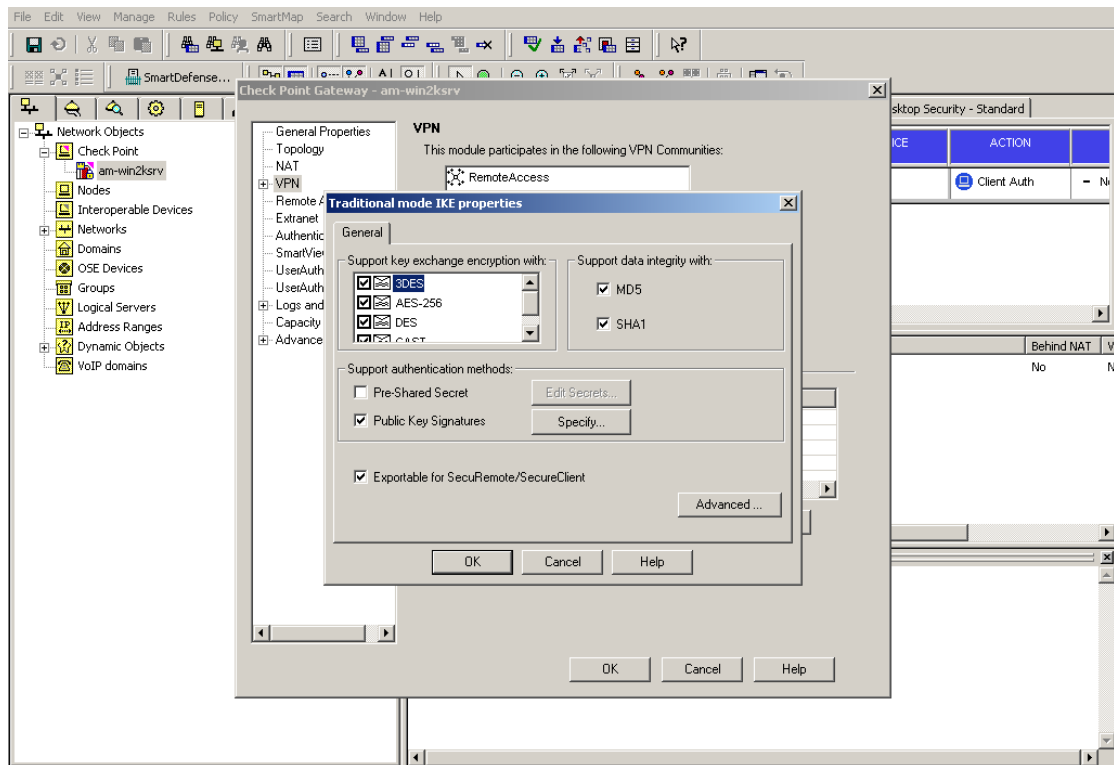


Figure 72: SmartDashboard: Traditional mode IKE Properties

➔ Tick 'Public Key Signatures' and click on **Specify**

In the *Additional certificates* dialog, select the option “The Gateway must use a certificate issued by this Certificate Authority”, and from the dropdown menu select the (newly created) Microsoft CA:

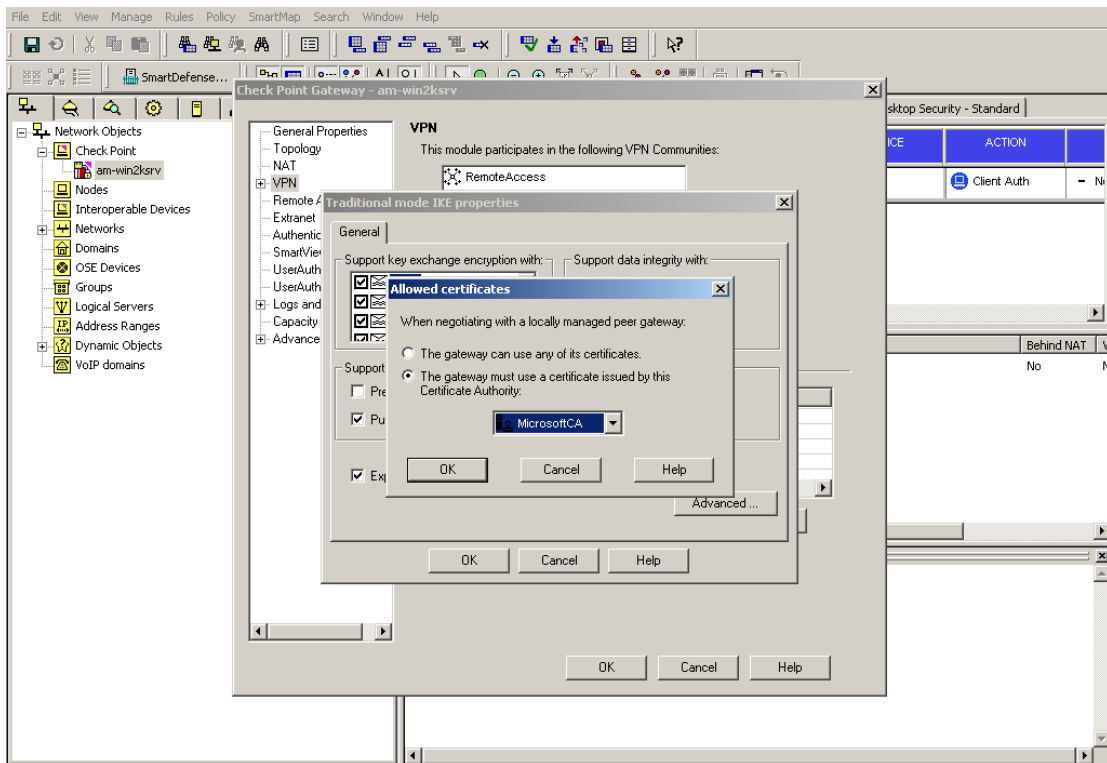


Figure 73: SmartDashboard: Allowed certificates

➔ Click **OK**

In the *Traditional mode IKE properties* dialog, tick the checkbox for ‘Exportable for SecuRemote/SecureClient’:

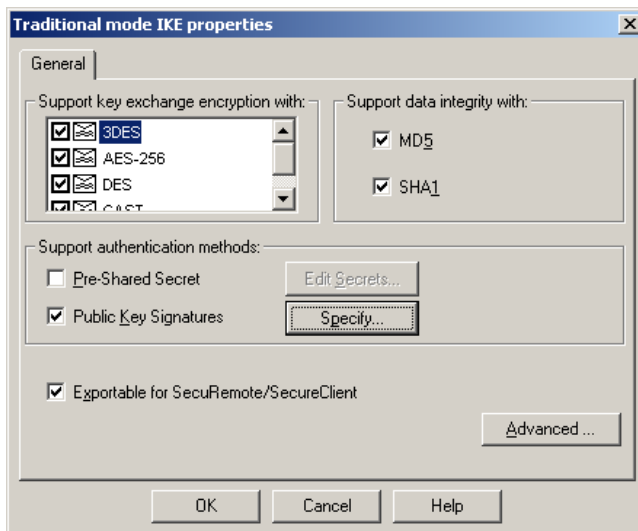


Figure 74: Traditional mode IKE Properties

➔ Click **OK** and close all windows

Next, go to **Policy > Global Properties**

Select **Authentication** tab and de-select “Authenticate Internal users with this suffix only” (as below):

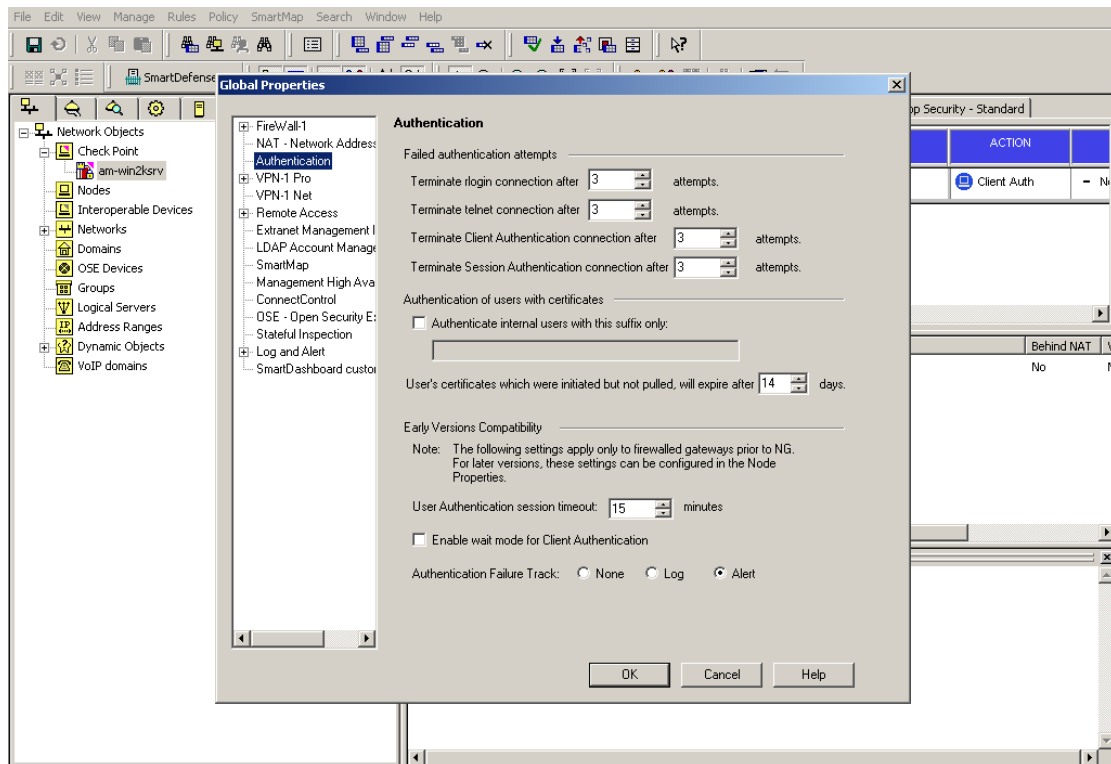


Figure 75: SmartDashboard: Global Properties

➔ Click **OK** and save your policy.

Now you will need to create a new user in your user database.

4.7 Create new user

The seventh step is to create a new user in your user database.

Go to **Manage > Users and Administrators** to open the *Users and Administrators* dialog:

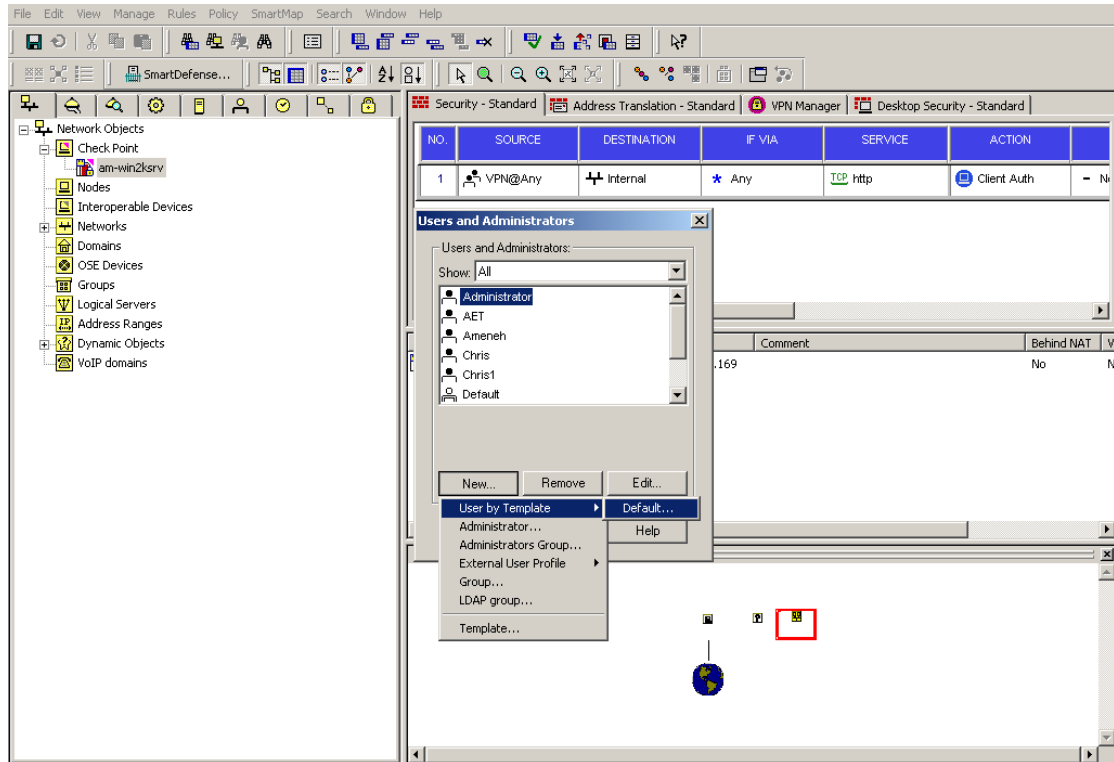


Figure 76: SmartDashboard: Users and Administrators

➔ Click on **New > User by Template > Default** (as above)

In the *General* tab, enter a user name (e.g. 'Test' as below):

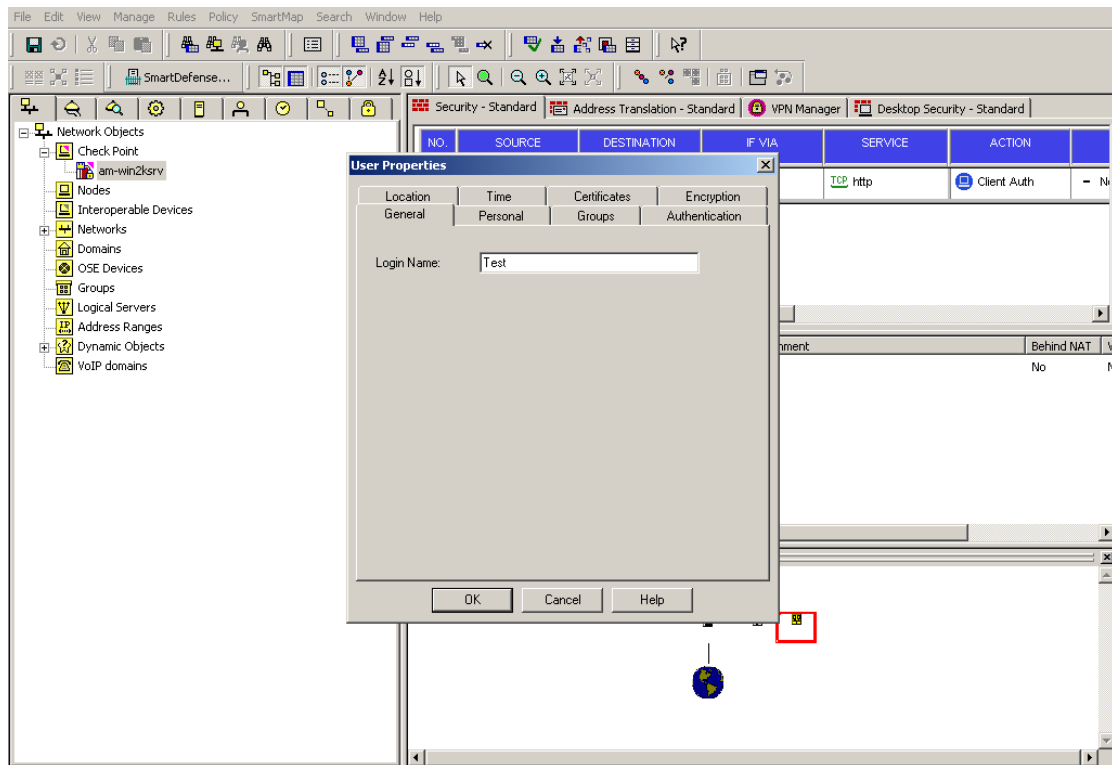


Figure 77: SmartDashboard: User Properties: General

➔ Select the *Groups* tab

In the *Groups* tab, add the user to a previously created group by selecting the user and clicking **Add**>:

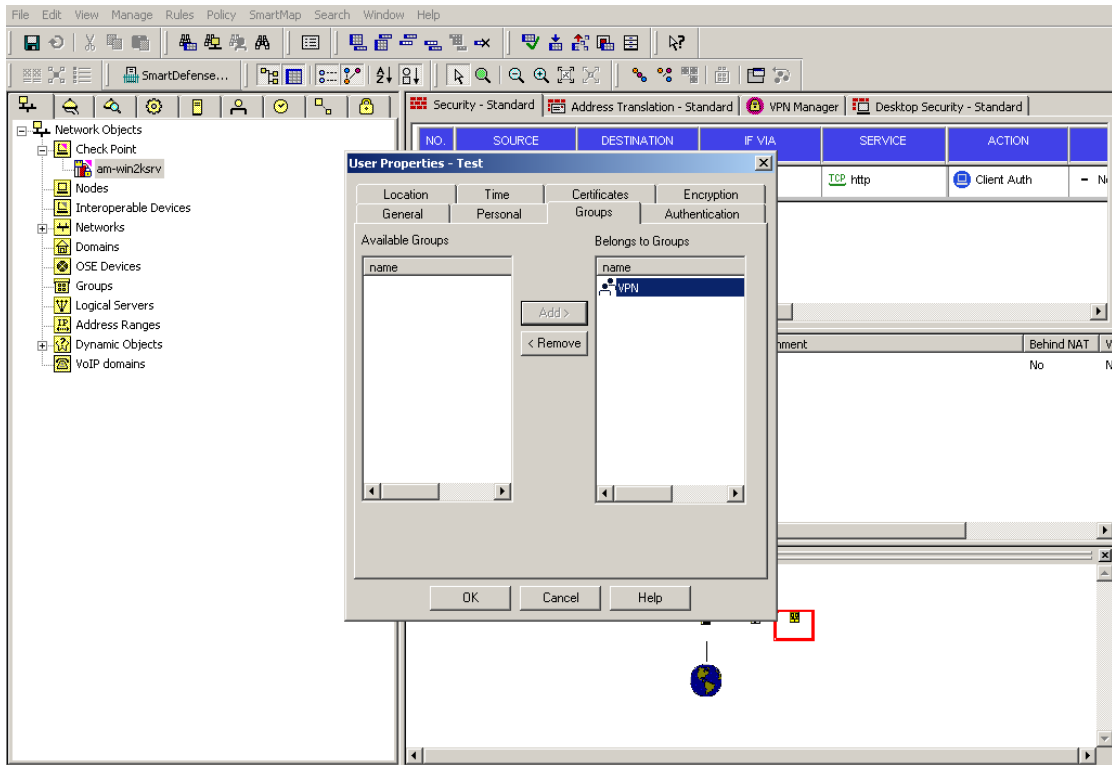


Figure 78: SmartDashboard: User Properties: Groups

➔ Select the *Authentication* tab

In the *Authentication* tab, select **Undefined** as the Authentication Scheme:

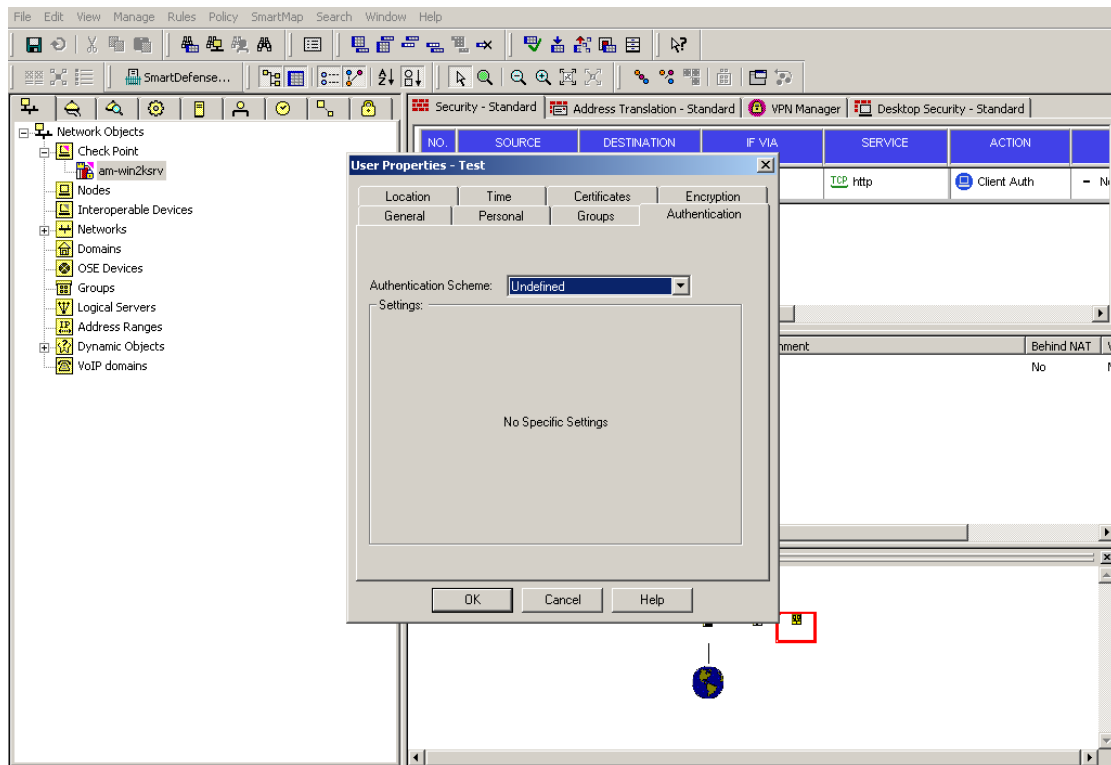


Figure 79: SmartDashboard: User Properties: Authentication

➔ Select the *Encryption* tab

In the *Encryption* tab, under 'Client Encryption Methods', select **IKE** as the Client Encryption Method:

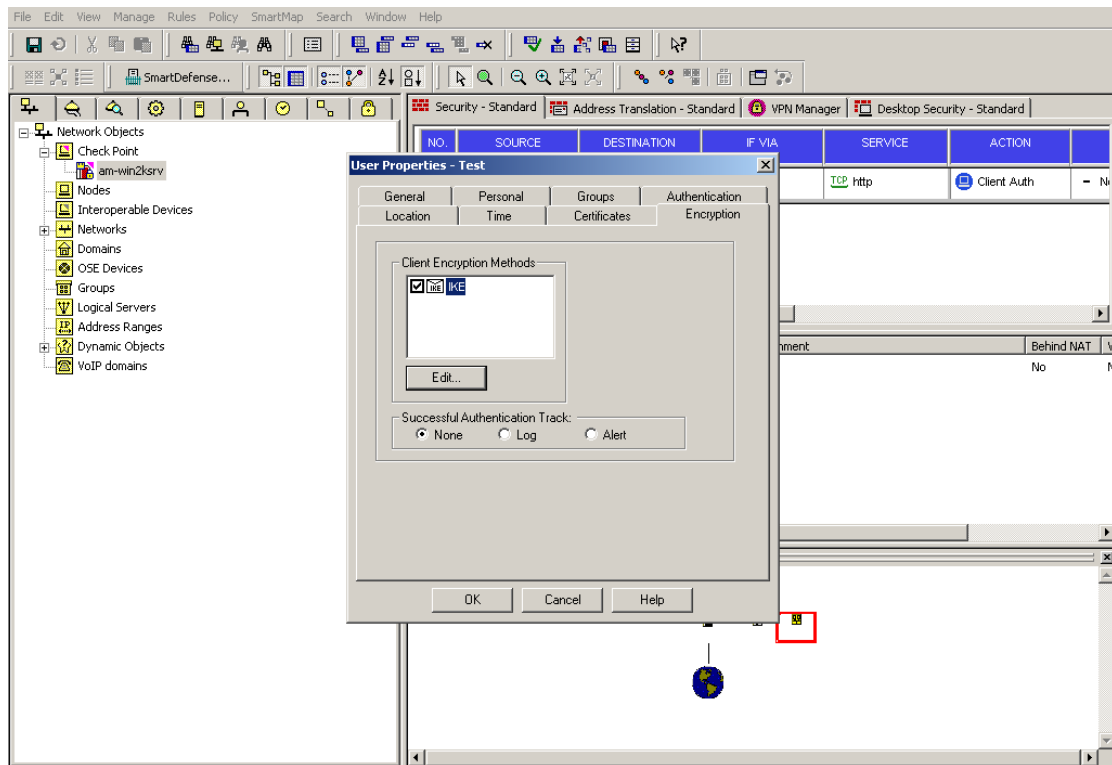


Figure 80: SmartDashboard: User Properties: Encryption

➔ Click on **Edit** and select Public Key in the *IKE phase 2 Properties* dialog

Click **OK** (twice) to close the *IKE phase 2 Properties* dialog and the *User Properties* dialog and install the user database, by clicking on the **install** button:

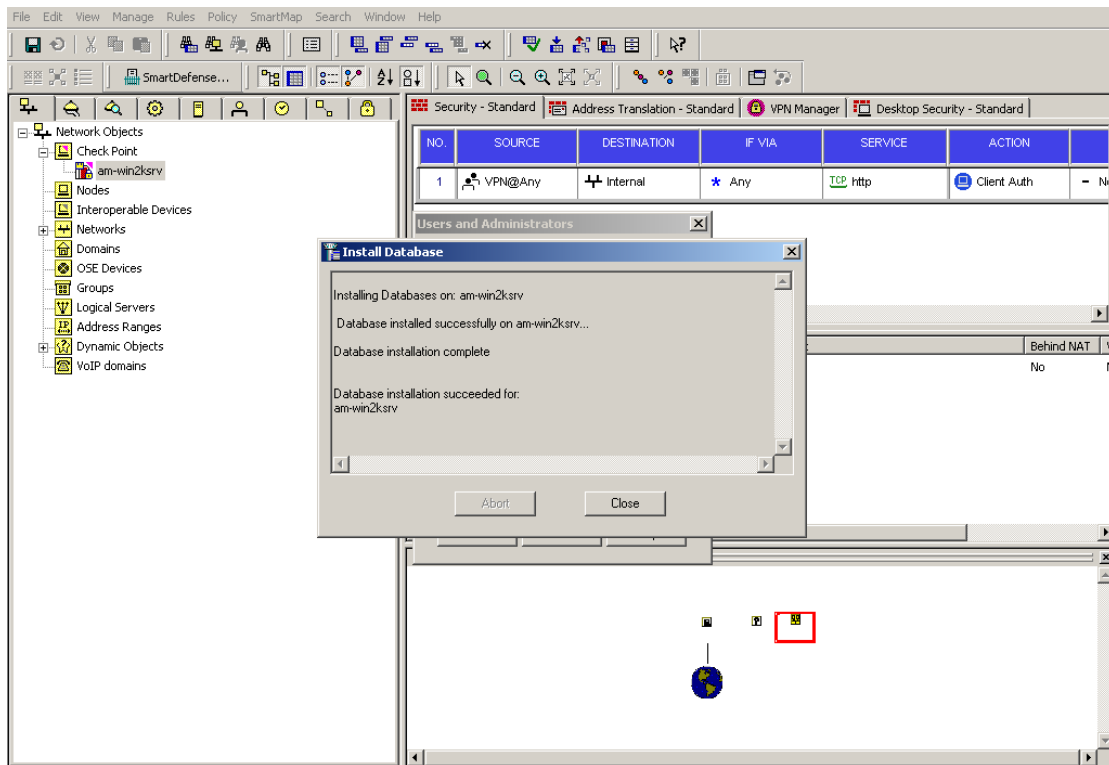


Figure 81: SmartDashboard: Install Database

➔ Close all windows and save the policy.

➔ Add a rule to enable communication between the group of users and the Gateway. Select 'Client Encrypt' as the action in the rule.

Note that when modifying and compiling rules in the Check Point VPN-1 / FireWall-1 SmartDashboard, you will need to select **Update Site** from the **Sites** menu of the Check Point VPN-1 SecuRemote / SecureClient (if such a site is already created).

➔ Select Install from the **Policy** menu to install the Security Policy on the Gateway.

Now you are ready to obtain a certificate on your SafeSign token, as described in [Chapter 3](#).

Index of Notes

Cancel PIN	7
Certificate Chain	10
Import CA certificates	15
Incorrect PIN	7
Key Size Error	18
No Token	5
Note	13, 14, 29
PIN / PUK length	17
Root Certificate Store	21
Set the label of the ID on the token to a non default-value	16
Token Locked	8
Token out of Memory	18
Token Removed	9
Update Site	11
View Certificate	5
Wrong Certificate	10
Wrong Password	16